

Symantec™ Protection Center – Benutzerhandbuch

Version 2.0

Symantec™ Protection Center – Benutzerhandbuch

Die in diesem Handbuch beschriebene Software wird unter einer Lizenzvereinbarung zur Verfügung gestellt und darf nur gemäß den Bestimmungen dieser Vereinbarung verwendet werden.

Dokumentationsversion: 2.0

Rechtlicher Hinweis

Copyright © 2011 Symantec Corporation. Alle Rechte vorbehalten.

Symantec und das Symantec-Logo sind Marken oder eingetragene Marken der Symantec Corporation oder ihrer verbundenen Unternehmen in den USA und anderen Ländern. Andere Bezeichnungen können Marken anderer Rechteinhaber sein.

Das in diesem Dokument beschriebene Produkt wird zu Lizenzbedingungen ausgeliefert, die seine Verwendung, Vervielfältigung, Verteilung und Dekompilierung bzw. Rückübersetzung einschränken. Kein Teil dieses Dokuments darf in irgendeiner Form reproduziert werden, sofern nicht zuvor die schriftliche Genehmigung von Symantec Corporation und gegebenenfalls ihrer Lizenznehmer eingeholt wurde.

DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN VORAUSSETZUNGEN, DARSTELLUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHT-BEEINTRÄCHTIGUNG, SIND AUSGESCHLOSSEN, AUSSER IN DEM UMFANG, IN DEM SOLCHE HAFTUNGS AUSSCHLÜSSE ALS NICHT RECHTSGÜLTIG ANGESEHEN WERDEN. SYMANTEC CORPORATION IST NICHT VERANTWORTLICH FÜR INDIREKTE SCHÄDEN ODER FOLGESCHÄDEN IM ZUSAMMENHANG MIT DER BEREITSTELLUNG ODER VERWENDUNG DIESER DOKUMENTATION. DIE IN DIESER DOKUMENTATION ENTHALTENEN INFORMATIONEN KÖNNEN JEDERZEIT OHNE ANKÜNDIGUNG GEÄNDERT WERDEN.

Die lizenzierte Software und Dokumentation gelten als "kommerzielle Computersoftware" gemäß FAR Abs. 12.212 und unterliegen, je nach Anwendbarkeit, eingeschränkten Rechten gemäß der Definition in FAR Abs. 52.227-19 "Commercial Computer Software - Restricted Rights" und gemäß DFARS Abs. 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation" sowie etwaigen Nachfolgebestimmungen. Jegliche Verwendung, Modifizierung, Reproduktion, Vorführung, Demonstration oder Offenlegung der unter Lizenz bereitgestellten Software und Dokumentation durch die Regierung der USA erfolgt nur in Übereinstimmung mit dieser Vereinbarung.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.de>

Inhalt

Abschnitt 1	Protection Center – Überblick	11
Kapitel 1	Einführung in Protection Center	13
	Infos zu Protection Center	13
	Funktionsweise des Protection Center	14
	Weitere Informationen zu Protection Center	15
Kapitel 2	Erste Schritte mit Protection Center	17
	Erste Schritte mit Protection Center	17
	Zugriff auf Protection Center	18
	Erstes Einrichten von Protection Center	20
	Ändern des Kennworts für Ihr Benutzerkonto	21
	Ausloggen aus Protection Center	22
Abschnitt 2	Einrichten und Verwalten	23
Kapitel 3	Einführung in die Verwaltung von Protection Center	25
	Ausführung von Protection Center-Verwaltungsaufgaben	25
	Info zu Geschäftsanalysen in Protection Center	27
	Herunterfahren oder Neustarten von Protection Center	27
Kapitel 4	Arbeiten mit von Protection Center unterstützten Produkten	29
	Info zu unterstützten Produkten	29
	Integrieren unterstützter Produkte	30
	Hinzufügen eines unterstützten Produkts in Protection Center	32
	Erforderliche unterstützte Produkthost-Einstellungen	33
	Unterstützte erweiterte Produkthost-Einstellungen	33
	Erkennen unterstützter Produkte im Netzwerk	34
	Info zum Verwalten unterstützter Produkte	35
	Aktivieren eines unterstützten Produkts	37
	Deaktivieren eines unterstützten Produkts	38

Nicht verbundenes Produkt erneut aktivieren	39
---	----

Kapitel 5

Integrieren von Mail Security in Protection Center	41
Info zur Integration von Mail Security mit Protection Center	41
Integrieren von Mail Security in Protection Center	42
Aktivieren von Mail Security	44
Installieren des Mail Security-Plugins auf Mail Security-Servern	45
Installieren des Mail Security-Plugins unter Verwendung der Push-Methode	46
Installieren des Mail Security-Plugins unter Verwendung der Pull-Methode	47
Überwachen des Status von Mail Security-Vorgängen	49
Info zu den Vorgangsstatusinformationen	50
Upgrades des Mail Security-Plugins auf integrierten Mail Security-Servern	51
Deinstallieren des Mail Security-Plugins von einem Mail Security-Server	52

Kapitel 6

Verwalten von Protection Center-Benutzerkonten	55
Über Protection Center-Benutzerkonten	56
Info zum SPC_Admin-Konto	57
Einrichten von Protection Center-Benutzerkonten	57
Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung	58
"Active Directory und LDAP"-Servereinstellungen	59
Angeben des Basis-DN	61
Angeben des Filters für die Benutzersuche	62
Optionen für die Protection Center-Benutzerkontoverwaltung	63
Erstellen von Protection Center-Benutzerkonten	64
Ändern eines Protection Center-Benutzerkontos	66
Authentifizierungstypen für Protection Center-Benutzerkonten	67
Benutzerauthentifizierungseinstellungen für Protection Center (lokal)	68
Active Directory- und LDAP-Authentifizierungseinstellungen	69
Protection Center-Benutzerkontoberechtigungseinstellungen	70
Protection Center-Benutzerkontoberechtigungen	71
Unterstützte Produktzugriffsberechtigungseinstellungen	75
Löschen eines Protection Center-Benutzerkontos	76

Kapitel 7	Verwalten von Protection Center-Softwareupdates	77
	Infos zu Softwareupdates für Protection Center	77
	Verwalten von Protection Center-Softwareupdates	78
	Angabe des LiveUpdate-Servers	80
	LiveUpdate-Einstellungen	81
Kapitel 8	Sichern und Wiederherstellen von Protection Center	83
	Info zu Protection Center-Backup und -Wiederherstellung	83
	Planen von automatischen Backups	85
	Backup-Einstellungen	85
	Wiederherstellen von Protection Center	87
	Erstellen des Symantec Recovery Disk	90
	Testen des Symantec Recovery Disk	91
Kapitel 9	Konfigurieren der Protection Center-Einstellungen	93
	Protection Center-Konfigurationseinstellungen	93
	Zugreifen auf die Protection Center-Konfigurationseinstellungen	96
	Community-Statistik-Einstellungen	96
	Datums- und Uhrzeiteinstellungen	97
	E-Mail-Einstellungen	97
	Nachrichtenprotokollierungseinstellungen	99
	Netzwerkkonfigurationseinstellungen	100
	Proxy-Server-Einstellungen	100
	Datenbereinigungseinstellungen	102
Kapitel 10	Die Protection Center-Systemsteuerung	105
	Protection Center-Systemsteuerungsoptionen	105
	Zugreifen auf die Protection Center-Systemsteuerung	107
	Manuelles Aktualisieren der Protection Center-Software	107
	Ändern des Kennworts für das SPC_Admin-Konto	108
	Netzwerkeinstellungen angeben	109
	Windows-Betriebssystem aktivieren	111
Kapitel 11	Hilfe bei Problemen mit Protection Center	113
	Ressourcen zur Problembehebung in Protection Center	113
	Hilfe vom Symantec-Support	115

	Symantec-Support-Diagnoseoptionen	116
	Sammeln von Protection Center-Diagnosedaten	118
	Supportanfrageneinstellungen	120
	Speichern einer Diagnosedatei	122
	Senden einer Diagnosedatei an den Symantec-Support	123
Abschnitt 3	Sicherheitsmanagement	125
Kapitel 12	Einleitung zum Sicherheitsmanagement mit Protection Center	127
	Ausführung von Sicherheitsmanagement-Aufgaben in Protection Center	127
	Info zum Protection Center-Dashboard	129
	Zugriff auf die Verwaltungsschnittstelle eines unterstützten Produkts	131
Kapitel 13	Verwenden von Protection Center-Berichten	133
	Info zu Berichten	133
	Info zu Diagrammen	134
	Info zu Berichtsaktionen	135
	Info zu Berichtsfiltern	135
	Anzeigen eines Berichts	136
	Anwenden von Filtern auf einen Bericht	138
	Erstellen gespeicherter Berichte	139
	Löschen eines gespeicherten Berichts	141
	Konfigurieren der Verteilung eines Berichts	141
	Berichtsverwaltungseinstellungen	142
	Berichtsverteilungseinstellungen	143
	Info zu speziellen Berichten für Mail Security	144
Kapitel 14	Arbeiten mit Benachrichtigungen	147
	Info zu Benachrichtigungen	147
	Anzeigen und Verwalten von Benachrichtigungen	148
	Benachrichtigungsdetails	149
Kapitel 15	Arbeiten mit Arbeitsabläufen und Aufgaben	151
	Info zu Workflows	151
	Verwendung von Protection Center-Workflows	152
	Konfigurieren der Verwaltungseinstellungen für einen Workflow	154

Starten eines Workflows	154
Überwachen Ihrer Workflows und Aufgaben	155
Workflow-Details	156
Aufgabendetails	157
Reaktion auf eine Aufgabenzuweisung	158
Verfügbare Workflows in Protection Center	159
Quarantäneendgerät -Workflow	161
Workflow "Virendefinitionen auf Endgerät aktualisieren"	163
Workflow "Endgerät verschieben"	164
Workflow "Virendefinitionen und Scan-Endgerät aktualisieren"	164
"NationalThreatLevelMonitor" -Workflow	165
"ZeroDayVulnerabilityMonitor" -Workflow	166
Index	167

Protection Center – Überblick

- [Kapitel 1. Einführung in Protection Center](#)
- [Kapitel 2. Erste Schritte mit Protection Center](#)

Einführung in Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Infos zu Protection Center](#)
- [Funktionsweise des Protection Center](#)
- [Weitere Informationen zu Protection Center](#)

Infos zu Protection Center

Symantec Protection Center ist eine zentralisierte Sicherheitsmanagement-Anwendung. Unternehmen können neue Bedrohungen erkennen, Aufgaben nach Priorität ordnen und die zum Schutz mit brauchbaren Informationen benötigte Zeit verkürzen. Protection Center nutzt eine Kombination aus Prozessautomatisierung und Sicherheitsinformationsbeschaffung, damit Benutzer Vorfälle beheben und Schlüsselsysteme und Datenbestände proaktiv schützen können. Protection Center enthält Frühwarnungen aus dem Symantec Global Intelligence Network, eine der weltweit größten kommerziellen Cyber-Info-Communitys.

Protection Center hilft beim Verbessern der Sicherheit durch Bereitstellen folgender Funktionen:

- Eine zentrale Ansicht über Endgerät, Nachrichten und Sicherheitsprodukte anderer Hersteller durch Single Sign-On, Datenerfassung und Prozessautomatisierung.
- Produktübergreifende Berichterstellung mit Berichtsvorlagen zu Malware, E-Mail und Assets.

- Überwachen globaler Sicherheitsereignisse und frühe Warnung vor relevanten Bedrohungen
- Leistungsstarke Geschäftsanalysefunktionen für Analysen und Berichterstellungen zu den in Ihrer Umgebung verfügbaren Daten.
- Single Sign-On-Zugriff auf Sicherheitsprodukte von Symantec und anderer Hersteller.
- Korrelation lokaler Produktdaten mit globalen Cyber-Info-Daten.
- Automatisierung gängiger Sicherheitsvorgänge mit vorgefertigten Workflow-Vorlagen

Siehe ["Funktionsweise des Protection Center"](#) auf Seite 14.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Funktionsweise des Protection Center

Protection Center sammelt Informationen von den Produkten in Ihrer Umgebung sowie von Symantec Global Intelligence Network. Protection Center normalisiert die Daten und erstellt für jedes der einzelnen Produktereignisse Kontext. Die entsprechenden Aufgaben sind basierend auf jeder einzelnen Benutzerrolle priorisiert. Die Informationen und Aufgaben werden im Protection Center-Dashboard angezeigt, in dem Benutzer produktübergreifende Berichte generieren und Reparatur-Workflows für mehrere integrierte Produkte starten können. Protection Center bietet Single-Sign-On-Zugriff auf die integrierten Symantec- und die Drittanbieterprodukte.

Siehe ["Infos zu Protection Center"](#) auf Seite 13.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Protection Center führt die folgenden Hauptfunktionen aus:

- Sammelt Daten von den Sicherheitsprodukten und von Global Intelligence Network
- Korreliert lokale Produktdaten mit Global Intelligence-Daten
- Liefert Ereignisbenachrichtigungen basierend auf Benutzerrolle und Schweregrad
- Generiert produktübergreifende Berichte
- Erleichtert Workflow-Abläufe
- Bietet Single-Sign-On für die Sicherheitsprodukte in Ihrer Organisation

Siehe ["Info zu Benachrichtigungen"](#) auf Seite 147.

Siehe "Info zu Berichten" auf Seite 133.

Weitere Informationen zu Protection Center

Verschiedene Quellen enthalten Informationen zu Protection Center.

Tabelle 1-1 Weitere Informationen zu Protection Center

Element	Beschreibung
Protection Center-Webseite	Wichtige Informationen zu Protection Center und Links zur Dokumentation und zu anderen Ressourcen. Die Seite enthält auch Links zum Protection Center Appliance Creator-Programm, das zur Herstellung virtueller und physischer Appliances von Protection Center verwendet wird. Sie finden die Protection Center-Seite auf der Symantec-Website unter folgender URL: http://go.symantec.com/protection-center
<i>Symantec Protection Center – Erste Schritte</i>	Informationen zur Bereitstellung von Protection Center: Architektur, Anforderungen, Erstellen von Appliances und erstes Einrichten. Diese Informationen sind über die Protection Center-Seite auf der Symantec-Website im PDF-Format verfügbar.
<i>Handbuch zur Größenaufteilung und Skalierbarkeit von Symantec Protection Center</i>	Detaillierte Informationen zum Anpassen Ihrer Protection Center-Installation an die Bedürfnisse Ihres Unternehmens. Diese Informationen sind über die Protection Center-Seite auf der Symantec-Website im PDF-Format verfügbar.
<i>Symantec Protection Center-Benutzerhandbuch und Symantec Protection Center-Hilfe</i>	Ausführliche Informationen zur Anwendung von Protection Center, einschließlich Verwaltung und Sicherheitsmanagement. Dieses Benutzerhandbuch ist über die Protection Center-Seite auf der Symantec-Website im PDF-Format verfügbar. Diese Hilfe ist im HTML-Format über Protection Center verfügbar. Sie können auf die Informationen über die Option "Hilfe" in der oberen rechten Ecke der Protection Center-Schnittstelle zugreifen.
<i>Versionshinweise zu Symantec Protection Center</i>	Die aktuellsten Informationen zu Protection Center-Funktionen, bekannte sowie gelöste Probleme. Diese Informationen sind über die Protection Center-Seite auf der Symantec-Website im HTML-Format verfügbar. http://go.symantec.com/protection-center

Siehe "Infos zu Protection Center" auf Seite 13.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Erste Schritte mit Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Erste Schritte mit Protection Center](#)
- [Zugriff auf Protection Center](#)
- [Erstes Einrichten von Protection Center](#)
- [Ändern des Kennworts für Ihr Benutzerkonto](#)
- [Ausloggen aus Protection Center](#)

Erste Schritte mit Protection Center

Jeder Protection Center-Benutzer hat gewöhnlich eine von zwei Rollen: Administrator oder Sicherheits-Manager. Ein Protection Center-Administrator erstellt die Protection Center-Appliance, richtet sie ein und führt laufende Protection Center-Konfigurationsaufgaben durch.

Es gibt folgende Protection Center-Verwaltungsaufgaben:

- Ausführen der ersten Konfiguration von Protection Center
Siehe ["Erstes Einrichten von Protection Center"](#) auf Seite 20.
- Unterstützte Produkte integrieren
- Verwalten von Benutzern
- Konfigurieren der Einstellungen für LiveUpdate, Backup und Protection Center
- Konfigurieren von Workflows
- Überwachen der Protection Center-Leistung anhand von Berichten

- Überwachen der Benachrichtigungen bzgl. Hardware-, Software- und Leistungsproblemen und entsprechende Aktionen
- Beheben von Fehlern in Protection Center

Siehe "[Ausführung von Protection Center-Verwaltungsaufgaben](#)" auf Seite 25.

Ein Sicherheits-Manager verwendet Protection Center-Berichte und Dashboards, um den Sicherheitsstatus des Unternehmens zu überwachen, und behebt Sicherheitsprobleme.

Es gibt folgende Protection Center-Sicherheits-Management-Aufgaben:

- Überwachen des Sicherheitsstatus mit dem Protection Center-Dashboard
- Überwachen Sie den Status des Netzwerks und der Endgeräte mithilfe von Berichten
- Beheben von Sicherheitsprobleme auf Endgeräten durch das Ausführen von Workflows, die Sie von Berichten aus gestartet werden
- Verwalten von Produkte über Produktansichten

Siehe "[Ausführung von Sicherheitsmanagement-Aufgaben in Protection Center](#)" auf Seite 127.

Zugriff auf Protection Center

Sie greifen auf Protection Center unter Verwendung eines Webbrowsers auf einem Endgerät und eines Protection Center-Benutzerkontos zu. Falls Sie noch keine Protection Center-Benutzerkonten eingerichtet haben, verwenden Sie das vordefinierte Protection Center-Administratorkonto (SPC_Admin) und das Kennwort, das während der Appliance-Erstellung angegeben wurde.

Siehe "[Info zum SPC_Admin-Konto](#)" auf Seite 57.

Siehe "[Über Protection Center-Benutzerkonten](#)" auf Seite 56.

Wenn Sie sich bei Protection Center unter Verwendung des vordefinierten Administratorkontos einloggen, wird das Dialogfeld "Erstes Einrichten" angezeigt. Im Dialogfeld "Erstes Einrichten" finden Sie Informationen zu den Einstellungen, die Sie konfigurieren müssen, damit Protection Center einsatzbereit ist. Sie können auf die Einstellungen direkt über die Links im Dialogfeld "Erstes Einrichten" zugreifen. Falls Sie sich mit einem anderen Protection Center-Benutzerkonto einloggen, gelangen Sie direkt zum Protection Center-Dashboard. Das Dashboard stellt eine umfassende Übersicht des Sicherheitsstatus Ihres Netzwerks bereit.

Siehe "[Erstes Einrichten von Protection Center](#)" auf Seite 20.

Nach dem Einloggen bei Protection Center befinden Sie sich in der Ansicht "Protection Center". Die Ansicht "Protection Center" ermöglicht den Zugriff auf

Protection Center-Berichte und -Konfigurationseinstellungen. Nach dem Integrieren von Produkten in Protection Center können Sie auch auf andere Produktansichten zugreifen. Über die Produktansicht können Sie ein bestimmtes Produkt verwalten.

Siehe "[Ändern des Kennworts für Ihr Benutzerkonto](#)" auf Seite 21.

Siehe "[Ausloggen aus Protection Center](#)" auf Seite 22.

Sie greifen auf Protection Center zu, indem Sie einen der folgenden Browser auf einem Endgerät verwenden, das Netzwerkzugriff auf Protection Center hat:

- Microsoft Internet Explorer 8
Kompatibilitätsmodus muss ausgeschaltet sein.
- Mozilla Firefox 3.5
- Safari 4.x

Hinweis: Einige Produkte, die ihre Benutzeroberfläche in Protection Center integrieren, unterstützen nicht alle von Protection Center unterstützten Browser. Die vom Produkt unterstützten Browser finden Sie in der Dokumentation des jeweiligen Produkts.

Eine aktuelle Liste von Symantec- und Drittanbieterprodukten, die mit Protection Center integrierbar sind, finden Sie auf der Protection Center-Seite der Symantec-Website. Die Protection Center-Seite befindet sich unter folgender URL:

<http://go.symantec.com/protection-center>

Protection Center erfordert außerdem eine Bildschirmauflösung von mindestens 1024x768 Pixeln.

Protection Center kann bis zu zehn gleichzeitig eingeloggte Benutzer unterstützen.

Wenn Sie mehrere gleichzeitig eingeloggte Benutzer verwenden möchten, müssen Sie eventuell Änderungen an Ihrer Protection Center-Installation vornehmen. Weitere Informationen finden Sie im Handbuch zur Größenaufteilung und Skalierbarkeit von Symantec Protection Center.

Hinweis: Da Protection Center ein selbstsigniertes Sicherheitszertifikat verwendet, wird jedes Mal, wenn Sie auf Protection Center zugreifen, eine Zertifikatsfehlermeldung angezeigt, bis Sie das Zertifikat einem vertrauenswürdigen Zertifikatspeicher hinzufügen.

So greifen Sie auf Protection Center zu

- 1
- Rufen Sie auf einem Endgerät mit einem unterstützten Webbrowser folgende Seite auf:

https://Name_der_Protection_Center_Appliance/Symantec
- 2
- Geben Sie Ihre Protection Center-Identifikationsdaten in das Login-Dialogfeld ein und klicken Sie auf "Einloggen".

Erstes Einrichten von Protection Center

Bevor Benutzer mit Protection Center beginnen können, muss sich der Protection Center-Administrator (SPC_Admin) bei Protection Center einloggen und erste Aufgabensetups durchführen. Wenn Sie sich bei Protection Center unter Verwendung des vordefinierten Administratorkontos einloggen, wird das Dialogfeld zum ersten Einrichten angezeigt. In diesem Dialogfeld finden Sie Informationen zu den Einstellungen, die Sie konfigurieren müssen, damit Protection Center einsatzbereit ist.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Siehe ["Zugriff auf Protection Center"](#) auf Seite 18.

Siehe ["Ausführung von Protection Center-Verwaltungsaufgaben"](#) auf Seite 25.

Die folgende Tabelle beschreibt den Prozess für die Ausführung des ersten Einrichtens von Protection Center.

Tabelle 2-1

Prozess für die Ausführung des ersten Einrichtens von Protection Center

Schritt	Aufgabe	Beschreibung
Schritt 1	Unterstützte Produkte integrieren	Integrieren Sie eines der unterstützten Produkte von Protection Center, die auf Ihrem Netzwerk verfügbar sind. Siehe "Integrieren unterstützter Produkte" auf Seite 30.
Schritt 2	Benutzerkonten einrichten	Richten Sie die erforderlichen Protection Center-Benutzerkonten ein. Siehe "Einrichten von Protection Center-Benutzerkonten" auf Seite 57.
Schritt 3	E-Mail-Einstellungen konfigurieren	Richten Sie den E-Mail-Server ein, den Protection Center für E-Mail-Benachrichtigungen und zum Verteilen von berichten verwenden soll. Richten Sie außerdem die E-Mail-Adresse des Administrators ein, der die Benachrichtigungen von Protection Center erhalten soll. Siehe "E-Mail-Einstellungen" auf Seite 97.

Schritt	Aufgabe	Beschreibung
Schritt 4	Proxy-Server einrichten	Geben Sie einen HTTP-Proxy-Server für Protection Center an, wenn Ihr Unternehmen einen HTTP-Proxy verwendet. Siehe " Proxy-Server-Einstellungen " auf Seite 100.
Schritt 5	Protection Center einrichten, um Community-Statistik-Daten zu sammeln und an Symantec zu senden.	Aktivieren Sie die Sammlung und das Senden von Diagnosedaten und anonymen Verwendungsdaten an Symantec. Obgleich die Verwendung dieser Funktion optional ist, sollten Sie sie verwenden, damit Symantec bessere Produktqualität und erweiterten Support gewähren kann. Siehe " Community-Statistik-Einstellungen " auf Seite 96.

Ändern des Kennworts für Ihr Benutzerkonto

Symantec empfiehlt, dass Sie das Kennwort Ihres Protection Center-Benutzerkontos in regelmäßigen Abständen ändern, um die Sicherheit Ihres Benutzerkontos zu gewährleisten. Wenn Ihr Protection Center-Benutzerkonto lokal authentifiziert wird, können Sie das Kennwort in Protection Center jederzeit ändern. Wenn Ihr Benutzerkonto Active Directory- oder LDAP-Authentifizierung verwendet, müssen Sie Ihr Kennwort außerhalb von Protection Center ändern.

Siehe "[Erste Schritte mit Protection Center](#)" auf Seite 17.

Siehe "[Zugriff auf Protection Center](#)" auf Seite 18.

Bei Änderungen an Kennwörtern von Administratorkonten können Dienste für andere eingeloggte Benutzer unterbrochen werden.

Ein lokales Protection Center-Kennwort muss aus mindestens acht Zeichen bestehen und mindestens drei der folgenden Angaben enthalten:

- Alphabetische Großbuchstaben (A bis Z)
- Alphabetische Unicode-Zeichen, die weder Großbuchstaben (A bis Z) noch Kleinbuchstaben (a bis z) sind
- Numerisches Zeichen (0 bis 9)
- Nicht alphanumerische Zeichen (~!@#\$\$%^&* _-+=`|\(){}[];:"'<>.,?/)

So ändern Sie Ihr Benutzerkontokennwort

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Kennwortänderung".
- 2 Geben Sie auf der Kennwortänderungsseite im Feld "Aktuelles Kennwort" Ihr ursprüngliches Kennwort ein.

- 3 Geben Sie im Feld "Neues Kennwort" das neue Kennwort ein, das Sie für Ihr Protection Center-Benutzerkonto verwenden möchten.
- 4 Geben Sie im Feld "Neues Kennwort bestätigen" das neue Kennwort ein, um die Änderung zu überprüfen.
- 5 Klicken Sie auf "Änderungen speichern".

Es kann bis zu einer Minute dauern, bis Kennwortänderungen wirksam werden.

Ausloggen aus Protection Center

Wenn Sie sich aus der Protection Center-Schnittstelle ausloggen, werden Sie aus Protection Center ausgeloggt. Außerdem werden Sie aus allen unterstützten Produkten ausgeloggt, mit denen Sie verbunden sind.

Ihre aktuelle Ansicht, bei der es sich um eine Protection Center-Seite oder eine Produktansicht handeln kann, wird zwischen Sitzungen beibehalten. Wenn Sie sich wieder einloggen, wird automatisch die gleiche Ansicht wiederhergestellt.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Siehe ["Zugriff auf Protection Center"](#) auf Seite 18.

So loggen sich aus Protection Center aus

- ◆ Klicken Sie in Protection Center rechts oben im Headerbereich auf "Ausloggen".

Einrichten und Verwalten

- Kapitel 3. Einführung in die Verwaltung von Protection Center
- Kapitel 4. Arbeiten mit von Protection Center unterstützten Produkten
- Kapitel 5. Integrieren von Mail Security in Protection Center
- Kapitel 6. Verwalten von Protection Center-Benutzerkonten
- Kapitel 7. Verwalten von Protection Center-Softwareupdates
- Kapitel 8. Sichern und Wiederherstellen von Protection Center
- Kapitel 9. Konfigurieren der Protection Center-Einstellungen
- Kapitel 10. Die Protection Center-Systemsteuerung
- Kapitel 11. Hilfe bei Problemen mit Protection Center

Einführung in die Verwaltung von Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Ausführung von Protection Center-Verwaltungsaufgaben](#)
- [Info zu Geschäftsanalysen in Protection Center](#)
- [Herunterfahren oder Neustarten von Protection Center](#)

Ausführung von Protection Center-Verwaltungsaufgaben

Wenn Sie der Protection Center-Administrator sind, sollten Sie mit Verwaltungsaufgaben vertraut sein, bevor Sie Protection Center zum ersten Mal ausführen. Wenn Sie sich zum ersten Mal einloggen, werden Sie aufgefordert, einige Erstkonfigurationen in Protection Center durchzuführen. Nachdem Sie das Einrichten von Protection Center durchgeführt haben, können Sie zusätzliche Verwaltungsaufgaben durchführen.

Siehe "[Erste Schritte mit Protection Center](#)" auf Seite 17.

Die folgende Tabelle beschreibt den Prozess für die Ausführung von Protection Center-Verwaltungsaufgaben.

Tabelle 3-1 Prozess für die Ausführung von Protection Center-Verwaltungsaufgaben

Schritt	Aufgabe	Beschreibung
Schritt 1	Loggen Sie sich bei Protection Center ein.	Greifen Sie auf Protection Center über die Protection Center-Schnittstelle zu. Normalerweise loggen Sie sich bei Protection Center unter Verwendung des vordefinierten SPC_Admin-Konten ein. Siehe " Zugriff auf Protection Center " auf Seite 18.
Schritt 2	Führen Sie das erste Einrichten von Protection Center durch.	Schließen Sie die Aufgaben des ersten Einrichtens ab, die für die Verwendung von Protection Center erforderlich sind. Siehe " Erstes Einrichten von Protection Center " auf Seite 20. Optional können Sie die Geschäftsanalysen in Protection Center so konfigurieren, dass sie mit den in Ihrer Umgebung verfügbaren Daten funktionieren. Siehe " Info zu Geschäftsanalysen in Protection Center " auf Seite 27.
Schritt 3	Konfigurieren Sie Software-Update-Einstellungen.	Konfigurieren Sie Symantec LiveUpdate, um regelmäßig nach Updates für Protection Center-Softwarekomponenten zu suchen. Siehe " Infos zu Softwareupdates für Protection Center " auf Seite 77.
Schritt 4	Konfigurieren Sie Backup-Einstellungen.	Konfigurieren Sie Symantec Backup Exec System Recovery, um regelmäßige Backups von Protection Center-Daten und -Systemdateien zu erstellen. Siehe " Info zu Protection Center-Backup und -Wiederherstellung " auf Seite 83.
Schritt 5	Passen Sie Protection Center für Ihre Umgebung an.	Ändern Sie die Konfigurationseinstellungen, damit Protection Center in Ihrer bestimmten Umgebung funktionieren kann und um sicherzustellen, dass es die Bedürfnisse Ihres Unternehmens erfüllt. Siehe " Protection Center-Konfigurationseinstellungen " auf Seite 93.
Schritt 6	Konfigurieren Sie die Workflows, mit denen Sie Aktionen auf bestimmten Endgeräten durchführen können.	Konfigurieren Sie jeden Workflow, um den Anforderungen Ihres Unternehmens gerecht zu werden. Nachdem der Protection Center-Administrator diese Aufgabe durchführt, kann der Sicherheitsmanager die Workflows dann verwenden, um alle Sicherheitsprobleme zu lösen, die in Ihrer Umgebung ermittelt werden. Siehe " Info zu Workflows " auf Seite 151.
Schritt 7	Führen Sie die laufende Integration von zusätzlichen Produkten mit Protection Center durch.	Integrieren Sie zusätzliche unterstützte Produkte, wenn sie auf Ihrem Netzwerk verfügbar sind. Siehe " Integrieren unterstützter Produkte " auf Seite 30.

Schritt	Aufgabe	Beschreibung
Schritt 8	Führen Sie die laufende Installation von Benutzerkonten durch.	Richten Sie nach Bedarf zusätzliche Protection Center-Benutzerkonten ein. Siehe " Einrichten von Protection Center-Benutzerkonten " auf Seite 57.
Schritt 9	Überwachen Sie kontinuierlich den Status Ihres Netzwerk- und Computermfelds.	Überwachen Sie den Status Ihrer Netzwerk- und Endgerätaggebung, indem Sie die Berichte verwenden, die spezifische Daten für Protection Center enthalten. Siehe " Info zu Berichten " auf Seite 133.
Schritt 10	Führen Sie die laufende Identifizierung und Aktionen als Reaktion auf Probleme mit Hardware, Software und Leistung aus.	Identifizieren Sie und reagieren Sie auf Hardware, Software und Performanceprobleme durch Benachrichtigungen. Eine Benachrichtigung ist eine Meldung, die Sie über ein Ereignis informiert, das aufgetreten ist. Protection Center generiert Benachrichtigungen, wenn Sie auf Probleme aufmerksam gemacht werden müssen. Siehe " Info zu Benachrichtigungen " auf Seite 147.
Schritt 11	Führen Sie gegebenenfalls eine Fehlerbehebung in Protection Center durch.	Sammeln Sie Diagnoseinformationen aus Protection Center und senden Sie sie für Support-Zwecke an Symantec. Siehe " Ressourcen zur Problembehebung in Protection Center " auf Seite 113. Siehe " Hilfe vom Symantec-Support " auf Seite 115.

Info zu Geschäftsanalysen in Protection Center

Die Geschäftsanalysefunktion in Protection Center bietet mehrdimensionale Analysen und zuverlässige grafische Berichterstellung. Diese Funktion ermöglicht es Benutzern von Protection Center, Daten selbständig zu durchsuchen, ohne dafür fortgeschrittene Kenntnisse zu Datenbanken oder Berichterstellungs-Tools von Drittanbietern zu benötigen. So können Protection Center-Benutzer ihre Fragen schnell und einfach selbst beantworten.

Informationen zum Aktivieren von Geschäftsanalysen in Ihrer Umgebung finden Sie auf der Protection Center-Seite der Symantec-Website.

<http://go.symantec.com/protection-center>

Herunterfahren oder Neustarten von Protection Center

Sie können die Protection Center-Appliance bei Bedarf herunterfahren oder neu starten. Wenn Protection Center heruntergefahren wird, funktionieren die

unterstützten Produkte weiterhin normal. Sie können jedoch keine Produktdaten an Protection Center senden, bis es neu gestartet ist. Wenn Protection Center heruntergefahren ist, speichern die unterstützten Produkte ihre Daten lokal. Wenn Protection Center neu gestartet wird, sammelt es automatisch alle "verpassten" Daten aus den unterstützten Produkten. Durch das lokale Speichern der Daten stellen integrierte Produkte sicher, dass Protection Center immer einen vollständigen Satz Daten für Berichte und Dashboards sammeln kann.

Siehe "[Ausführung von Protection Center-Verwaltungsaufgaben](#)" auf Seite 25.

Siehe "[Zugriff auf Protection Center](#)" auf Seite 18.

So fahren Sie Protection Center herunter oder starten es neu

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Herunterfahren".
- 2 Wählen Sie auf der Seite zum Herunterfahren der Appliance die entsprechende Option aus.

Herunterfahren	Verwenden Sie diese Option, wenn Sie Hardware austauschen oder die Appliance physisch verschieben müssen.
Neustart	Verwenden Sie diese Option, nachdem Sie Konfigurationsänderungen vorgenommen oder Appliance-Komponenten über LiveUpdate Upgrade aktualisiert haben.

- 3 Klicken Sie auf "Weiter".

Arbeiten mit von Protection Center unterstützten Produkten

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu unterstützten Produkten](#)
- [Integrieren unterstützter Produkte](#)
- [Hinzufügen eines unterstützten Produkts in Protection Center](#)
- [Erforderliche unterstützte Produkthost-Einstellungen](#)
- [Unterstützte erweiterte Produkthost-Einstellungen](#)
- [Erkennen unterstützter Produkte im Netzwerk](#)
- [Info zum Verwalten unterstützter Produkte](#)
- [Aktivieren eines unterstützten Produkts](#)
- [Deaktivieren eines unterstützten Produkts](#)
- [Nicht verbundenes Produkt erneut aktivieren](#)

Info zu unterstützten Produkten

Mithilfe von Protection Center können Sie mehrere Sicherheitsprodukte für zentrale Sicherheitsverwaltung zusammenführen. Die Produkte, die mit Protection Center funktionieren oder darin integrieren sind, sind als unterstützte Produkte in Protection Center bekannt.

Siehe "[Integrieren unterstützter Produkte](#)" auf Seite 30.

Unterstützte Produkte können mit Protection Center in einem oder beiden der folgenden Methoden integrieren:

- **Datenanzusammenfassung**
Protection Center sammelt Daten von den unterstützten Produkten und bündelt die Daten, um produktübergreifende Berichte zu erstellen. Protection Center erhält Benachrichtigungen von den unterstützten Produkten und zeigt diese an.
- **Produktverwaltung**
Protection Center zentralisiert die Verwaltung von unterstützten Produkten. Mithilfe von Protection Centers können Sie auf mehrere Produkte über eine einzelne Schnittstelle zugreifen.

Weitere Informationen zu unterstützten Produkten erhalten Sie unter *Symantec Protection Center-Erste Schritte*. Sie können auf das Handbuch über die Protection Center-Seite auf der Symantec-Website zugreifen. Eine vollständige Liste von unterstützten Produkten finden Sie auf der Protection Center-Seite auf der Symantec-Website. Die Protection Center-Seite befindet sich unter folgender URL:

<http://go.symantec.com/protection-center>

Integrieren unterstützter Produkte

Ein unterstütztes Produkt muss manuell integriert werden, bevor es mit Protection Center verwendet werden kann. Wenn das Produkt Datenintegration unterstützt, kann es Daten freigeben und Sicherheitsbenachrichtigungen an Protection Center senden. Wenn das Produkt Benutzerschnittstellenintegration unterstützt, können Sie das Produkt über Protection Center verwalten.

Siehe "[Info zu unterstützten Produkten](#)" auf Seite 29.

Siehe "[Zugriff auf die Verwaltungsschnittstelle eines unterstützten Produkts](#)" auf Seite 131.

Weitere Informationen zum Integrieren bestimmter unterstützter Produkte finden Sie in der vollständigen Liste unterstützter Produkte auf der Protection Center-Seite der Symantec-Website. Die Liste unterstützter Produkte enthält Links zu den entsprechenden Informationen über jedes Produkt. Die Protection Center-Seite befindet sich unter folgender URL:

<http://go.symantec.com/protection-center>

Hinweis: Sie können Symantec Mail Security für Microsoft Exchange (Mail Security) in Protection Center integrieren. Der in diesem Abschnitt beschriebene Integrationsvorgang gilt jedoch nicht für Mail Security.

Siehe "[Integrieren von Mail Security in Protection Center](#)" auf Seite 42.

Die folgende Tabelle beschreibt den Vorgang zum Integrieren unterstützter Produkten in Protection Center.

Tabelle 4-1 Integrieren unterstützter Produkten

Schritt	Aufgabe	Beschreibung
Schritt 1	Hinzufügen der unterstützten Produkte	Sie können unterstützte Produkte beim ersten Einrichten hinzufügen, wenn Sie sich zum ersten Mal bei Protection Center einloggen. Sie können unterstützte Produkte auch später auf der Produktverwaltungsseite hinzufügen. Siehe " Hinzufügen eines unterstützten Produkts in Protection Center " auf Seite 32.
Schritt 2	(Optional) Erkennen unterstützter Produkte	Sie können Protection Center so konfigurieren, dass unterstützte Produkte automatisch erkannt werden, die im Netzwerk installiert sind. Siehe " Erkennen unterstützter Produkte im Netzwerk " auf Seite 34.
Schritt 3	Aktivieren der unterstützten Produkte	Sie können die unterstützten Produkte aktivieren, die im Netzwerk verfügbar sind. Wenn mehrere Instanzen eines Produkts verfügbar sind, können Sie jede Produktinstanz einzeln aktivieren. Siehe " Info zum Verwalten unterstützter Produkte " auf Seite 35. Siehe " Aktivieren eines unterstützten Produkts " auf Seite 37.
Schritt 4	(Optional) Erneutes Aktivieren von Produkten, die von Protection Center getrennt wurden	Ein aktiviertes Produkt kann von Protection Center getrennt werden, wenn Probleme mit der Netzwerkverbindung auftreten oder Änderungen am Produkthost vorgenommen werden. Sie müssen das Verbindungsproblem beheben und das Produkt in Protection Center erneut aktivieren. Siehe " Nicht verbundenes Produkt erneut aktivieren " auf Seite 39.
Schritt 5	(Optional) Deaktivieren von Produkten, die nicht mehr über Protection Center verwaltet werden sollen	Sie können aktivierte Produkte deaktivieren, die Sie nicht mehr über Protection Center verwalten möchten. Siehe " Deaktivieren eines unterstützten Produkts " auf Seite 38.

Hinzufügen eines unterstützten Produkts in Protection Center

Sie können Protection Center ein unterstütztes Produkt hinzufügen. Das unterstützte Produkt muss auf Ihrem Netzwerk in einem Speicherort installiert werden, auf den Protection Center zugreifen kann.

Siehe ["Info zu unterstützten Produkten"](#) auf Seite 29.

Siehe ["Integrieren unterstützter Produkte"](#) auf Seite 30.

Siehe ["Info zum Verwalten unterstützter Produkte"](#) auf Seite 35.

So fügen Sie ein unterstütztes Produkt in Protection Center hinzu

- 1 In Protection Center haben Sie folgende Möglichkeiten:

So fügen Sie ein Produkt als Teil des ersten Einrichtens hinzu	Klicken Sie im Dialogfeld "Erstes Einrichten" unter "Produktintegration" auf "Produkte integrieren".
--	--

So fügen Sie ein Produkt von der Produktverwaltungsseite hinzu	Klicken Sie im Admin -Menü auf "Unterstützte Produkte" und dann auf der Produktverwaltungsseite auf "Produkt hinzufügen".
--	---

- 2 Geben Sie im Dialogfeld "Produktinstanz hinzufügen und aktivieren" die entsprechenden Produktparameter an.

Siehe ["Erforderliche unterstützte Produkthost-Einstellungen"](#) auf Seite 33.

- 3 Wenn Sie einen bestimmten Tenant für ein Multi-Tenan-Produkt angeben möchten oder wenn der Produkthost nicht standardmäßige Konfigurationseinstellungen verwendet, klicken Sie auf "Erweiterte Optionen".

Geben Sie unter "Erweiterte Optionen" die entsprechenden Einstellungen an.

Siehe ["Unterstützte erweiterte Produkthost-Einstellungen"](#) auf Seite 33.

- 4 Klicken Sie auf "Aktivieren".

Wenn Protection Center die angegebenen Informationen geprüft hat, wird der Produkthost der Registerkarte "Aktivierte unterstützte Produkte" hinzugefügt.

Erforderliche unterstützte Produkthost-Einstellungen

Sie müssen diese Einstellungen angeben, wenn Sie ein unterstütztes Produkt zu Protection Center hinzufügen. Sie müssen den Ort des Produkthosts angeben und die Identifikationsdaten eines Administratorkontos für das Produkt liefern.

Siehe ["Hinzufügen eines unterstützten Produkts in Protection Center"](#) auf Seite 32.

Siehe ["Aktivieren eines unterstützten Produkts"](#) auf Seite 37.

Tabelle 4-2 Erforderliche unterstützte Produkthost-Einstellungen

Element	Beschreibung
Produkt	Gilt nur für das Dialogfeld "Produktinstanz hinzufügen und aktivieren". Enthält die Namen aller von Protection Center unterstützten Produkte in einer Dropdown-Liste.
Hostname	Gibt den Hostnamen oder die IP-Adresse der Produktinstanz an, die Sie hinzufügen möchten. Sie können IPv4- und IPv6-Adressen verwenden. In der Registerkarte "Verfügbare unterstützte Produkte" ist dieses Feld eine Dropdown-Liste, die die Namen aller verfügbaren Produktinstanzen enthält. Wenn nur eine einzelne Produktinstanz verfügbar ist, wird der Name im folgenden Format angezeigt: <i><Produktname (Tenantname)></i> .
"Administratorname"	Gibt den Benutzernamen eines Kontos an, das vollen Administratorzugriff auf das Produkt hat. Wenn Sie ein Domänenadministratorkonto verwenden möchten, müssen Sie die Domäne angeben. Beispiel: <i><Domäne>\<Benutzername></i> .
Administratorkennwort	Gibt das Kennwort des Administratorkontos an.
Erweiterte Optionen	Zeigt die Felder für erweiterte Produkthost-Einstellungen an. Siehe "Unterstützte erweiterte Produkthost-Einstellungen" auf Seite 33.

Unterstützte erweiterte Produkthost-Einstellungen

Sie müssen diese Einstellungen angeben, wenn Ihr Produkthost die Standardkonfigurationseinstellungen nicht verwendet. Außerdem müssen Sie diese Einstellungen angeben, wenn Sie einen bestimmten Tenant eines Produkts mit mehreren Tenants hinzufügen möchten.

Siehe ["Hinzufügen eines unterstützten Produkts in Protection Center"](#) auf Seite 32.

Siehe ["Aktivieren eines unterstützten Produkts"](#) auf Seite 37.

Siehe ["Erforderliche unterstützte Produkthost-Einstellungen"](#) auf Seite 33.

Die folgende Tabelle beschreibt die erweiterten unterstützten Produkthost-Einstellungen. Nur die für das ausgewählte Produkt relevanten Einstellungen werden angezeigt.

Tabelle 4-3 Unterstützte erweiterte Produkthost-Einstellungen

Element	Beschreibung
Tenant	Gilt nur für das Dialogfeld "Produktinstanz hinzufügen und aktivieren". Gibt den Tenant an, den Sie hinzufügen möchten.
Datenzufuhr-Port	Gibt den Port des Produkthosts an, der für die Datenzufuhr verwendet wird. Protection Center verwendet nach Aktivierung des unterstützten Produkts den angegebenen Port für alle sicheren Webdienstaufrufe. Hinweis: Wenn das Produkt einen einzigen konfigurierten Webdienst-Port hat, muss dieser Port sowohl für die Datenzufuhr als auch die Registrierung verwendet werden.
Datenflussname	Gibt das Administratorkonto an, das Berechtigung hat, auf die Datenzufuhr vom Produkt zuzugreifen. Standardmäßig entspricht der Benutzername dem Administratorkonto, das Sie in den erforderlichen Produkthost-Einstellungen angegeben haben.
Registrierungs-Port	Gibt den Port des Produkthosts an, der für das Aktivieren des Produkts in Protection Center verwendet wird. Protection Center verwendet den angegebenen Port für die ungesicherte Registrierung von Webdienstaufrufen zum Produkt. Hinweis: Wenn das Produkt einen einzigen konfigurierten Webdienst-Port hat, muss dieser Port sowohl für die Datenzufuhr als auch die Registrierung verwendet werden.
Konsolenport	Gibt den Port des Produkthosts an, der für den Zugriff auf die Benutzeroberfläche des Produkts (auch „Produktkonsole“) verwendet wird. Die Benutzeroberfläche des Produkts wird in Protection Center als Produktansicht angezeigt. Protection Center verwendet den angegebenen Port für Single-Sign-On-Webdienstaufrufe.
HTTPS verwenden	Gibt an, dass das Produkt HTTPS-Verbindungen mit Protection Center verwendet.

Erkennen unterstützter Produkte im Netzwerk

Sie können Protection Center so konfigurieren, dass im Netzwerk verfügbare unterstützte Produkte automatisch erkannt werden. Mithilfe des Erkennungsvorgangs können Sie einfach Produkte finden, die mit Protection

Center kompatibel sind. Außerdem werden alle aktivierten Produkte erkannt, die mehrere Mandanten unterstützen, d. h. Sie können zusätzliche Mandanten auf dem Produkthost aktivieren. Die aktivierten Produkte, die mehrere Mandanten nicht unterstützen, werden nicht erkannt.

Wenn Sie den Namen und die IP-Adresse eines Produkthost im Netzwerk bereits kennen, können Sie die Erkennung überspringen. Sie können das Produkt direkt hinzufügen und aktivieren, indem Sie die entsprechenden Informationen und gültige Administrator-Identifikationsdaten angeben. Wenn das Produkt aus Sicherheitsgründen nicht auf einen Protection Center-Erkennungsscan reagiert, müssen Sie das Produkt direkt aktivieren.

Siehe "[Info zu unterstützten Produkten](#)" auf Seite 29.

Siehe "[Hinzufügen eines unterstützten Produkts in Protection Center](#)" auf Seite 32.

Sie sollten die Produkterkennung das erste Mal nach der Installation von Protection Center ausführen. Der Erkennungsvorgang kann mehrere Stunden dauern.

Siehe "[Aktivieren eines unterstützten Produkts](#)" auf Seite 37.

Siehe "[Info zum Verwalten unterstützter Produkte](#)" auf Seite 35.

So erkennen Sie von Protection Center unterstützte Produkte im Netzwerk

- 1** Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Produkterkennung".
- 2** Auf der Seite "Produkterkennung" unter "IP-Auswahl für Erkennung:", geben Sie den IP-Adressbereich oder die gewünschten IP-Adressen ein.

Sie können IPv4- und IPv6-Adressen verwenden. Sie können mehrere IP-Adressen oder IP-Adressbereiche angeben, indem Sie die Einträge mit Kommas trennen. Sie können die IP-Adressen im Bereich durch einen Gedankenstrich trennen.
- 3** Unter "Zu erkennende unterstützte Produkte" wählen Sie die gewünschten Produkte aus.
- 4** Klicken Sie auf "Produkte erkennen".

Die Informationen zu den erkannten Produktinstanzen werden angezeigt. Die erkannten Produktinstanzen werden automatisch der Liste auf der Registerkarte "Verfügbare unterstützte Produkte" hinzugefügt.

Info zum Verwalten unterstützter Produkte

Die Produktverwaltungsseiten zeigt Informationen zu den Produkten an, die derzeit in Protection Center aktiviert sind und zu denen, die aktiviert werden

können. Sie können unterstützte Produkte Protection Center hinzufügen und verfügbare unterstützte Produkte aktivieren. Außerdem können Sie aktivierte Produkte deaktivieren und getrennte Produkte erneut aktivieren.

Siehe ["Info zu unterstützten Produkten"](#) auf Seite 29.

Siehe ["Integrieren unterstützter Produkte"](#) auf Seite 30.

Siehe ["Aktivieren eines unterstützten Produkts"](#) auf Seite 37.

Die folgende Tabelle beschreibt die Verwaltungsoptionen für unterstützte Produkte:

Tabelle 4-4 Verwaltungsoptionen für unterstützte Produkte

Option	Beschreibung
Produkt hinzufügen	Versucht, ein bestimmtes unterstütztes Produkt in Protection Center zu integrieren. Das unterstützte Produkt muss im Netzwerk in einem bekannten Speicherort installiert sein. Siehe "Hinzufügen eines unterstützten Produkts in Protection Center" auf Seite 32.
Produkt deaktivieren	Deaktiviert das auf der Registerkarte "Aktivierte unterstützte Produkte" in Protection Center ausgewählte Produkt. Siehe "Deaktivieren eines unterstützten Produkts" auf Seite 38.

Die Registerkarte "Verfügbare unterstützte Produkte" zeigt eine Übersicht über die unterstützten Produkte an, die im Netzwerk zwar verfügbar, aber derzeit nicht in Protection Center aktiviert sind. Sie können die gewünschten Produkte aktivieren, indem Sie die entsprechenden Administrator-Identifikationsdaten angeben.

Die Registerkarte "Aktivierte unterstützte Produkte" zeigt eine Übersicht über die derzeit in Protection Center aktivierten Produkte an. Jeder Produktbereich gibt den aktuellen Verbindungsstatus des Produkthost an: "Normal" oder "Fehler". Wenn auf einem Host ein Verbindungsfehler vorliegt, kann Protection Center keine Daten aus dem Produkt sammeln. Sie müssen das Verbindungsproblem beheben und das Produkt in Protection Center erneut aktivieren.

Siehe ["Nicht verbundenes Produkt erneut aktivieren"](#) auf Seite 39.

Wenn beide Registerkarten auf der Produktverwaltungsseite leer sind, kann einer der folgenden Zustände zutreffen:

- Sie haben die Produkterkennung noch nicht durchgeführt oder noch keine unterstützten Produkte hinzugefügt.
Siehe ["Erkennen unterstützter Produkte im Netzwerk"](#) auf Seite 34.
- Auf von Protection Center unterstützte Produkte kann vom Speicherort der Protection Center-Appliance aus nicht zugegriffen werden.

- Keine von Protection Center unterstützten Produkte sind im Netzwerk installiert.
- Keine von Protection Center unterstützten Produkte sind auf der Protection Center-Appliance installiert.

Die Produktliste hat auf beiden Registerkarten das gleiche Format: eine Liste von Produktbereichen, wobei jeder Bereich den Produktnamen und -version sowie die Anzahl der Hosts anzeigt. Jeder Host entspricht einer verfügbaren oder aktivierten Produktinstanz, entsprechend der Registerkarte. Sie können die einzelnen Produktbereiche erweitern, um Informationen zu jeder Produktinstanz anzuzeigen. Sie können eine einzelne Produktinstanz in der erweiterten Ansicht auswählen.

Aktivieren eines unterstützten Produkts

Wenn ein unterstütztes Produkt erkannt wird, wird die Produktinstanz der Liste der verfügbaren unterstützten Produkte hinzugefügt. Um dieses Produkt in Protection Center zu integrieren, müssen Sie den entsprechenden Produkthost in Protection Center aktivieren. Wenn Sie mehr als eine Instanz eines verfügbaren unterstützten Produkts (mehrere Produkthosts) haben, müssen Sie jede Produktinstanz separat aktivieren.

Siehe ["Info zu unterstützten Produkten"](#) auf Seite 29.

Siehe ["Erkennen unterstützter Produkte im Netzwerk"](#) auf Seite 34.

Wenn Sie ein Produkt aktivieren, müssen Sie möglicherweise die Identifikationsdaten eines Kontos angeben, das Administratorrechte für die Produktinstanz hat. Einige Produkte erfordern das Angeben von Identifikationsdaten jedoch nicht.

So aktivieren Sie ein unterstütztes Produkt

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Unterstützte Produkte".
- 2 Wählen Sie auf der Produktverwaltungsseite auf der Registerkarte "Verfügbare unterstützte Produkte" das zu aktivierende Produkt.
- 3 Klicken Sie im Produktbereich auf "Unterstütztes Produkt aktivieren".
Der Produktbereich wird erweitert, um die erforderlichen Produkthosteinstellungen anzuzeigen.
- 4 Geben Sie im Produktbereich die entsprechenden Einstellungen an.
Siehe ["Erforderliche unterstützte Produkthost-Einstellungen"](#) auf Seite 33.

- 5 Wenn Sie andere als Standardwerte für den Registrierungs-, Datenfeed- oder Konsolen-Port verwenden müssen, klicken Sie auf "Erweiterte Optionen".
Geben Sie unter "Erweiterte Optionen" die entsprechenden Einstellungen an.
Siehe "[Unterstützte erweiterte Produkthost-Einstellungen](#)" auf Seite 33.
- 6 Klicken Sie auf "Aktivieren".
Das Produktinstanzsymbol wird von der Registerkarte "Verfügbare unterstützte Produkte" entfernt und auf der Registerkarte "Aktivierte unterstützte Produkte" angezeigt.
- 7 Wenn eine Fehlermeldung angezeigt wird, klicken Sie auf "Weiter".
Sie müssen herausfinden, warum die Integration erfolglos war und das Problem beheben. Oft wurden nicht die richtigen Identifikationsdaten für das Administratorkonto eingegeben.

Deaktivieren eines unterstützten Produkts

Sie können ein unterstütztes Produkt deaktivieren, wenn Sie es nicht mehr von Protection Center aus verwalten möchten. Sie können es auch deaktivieren, falls Sie seine Identifikationsdaten für die Integration ändern möchten. Deaktivierte Produkte werden von der Registerkarte "Aktivierte unterstützte Produkte" entfernt. Für eine erneute Aktivierung zu einem späteren Zeitpunkt verwenden Sie den Standardprozess für das Aktivieren eines Produkts.

Siehe "[Info zu unterstützten Produkten](#)" auf Seite 29.

Siehe "[Integrieren unterstützter Produkte](#)" auf Seite 30.

Siehe "[Aktivieren eines unterstützten Produkts](#)" auf Seite 37.

Deaktivierte Produkte unterbrechen die Datenzufuhr und die Übermittlung von Benachrichtigungen an Protection Center. Außerdem können sie nicht mehr über Protection Center verwaltet werden. Wird ein Produkt deaktiviert, bewahrt Protection Center die vom Produkt gesendeten Benachrichtigungsdaten auf, löscht jedoch den Rest der Daten. Das Deaktivieren eines Produkts hat keine Auswirkungen auf das Produkt selbst und die darauf gespeicherten Daten.

So deaktivieren Sie ein unterstütztes Produkt

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Unterstützte Produkte".
- 2 Wählen Sie auf der Produktverwaltungsseite auf der Registerkarte "Aktivierte unterstützte Produkte" das Produkt, das Sie deaktivieren möchten.
Sind mehrere Produktinstanzen verfügbar, können Sie das Produktfenster erweitern und die entsprechende Produktinstanz auswählen.

- 3 Klicken Sie auf "Produkt deaktivieren".
- 4 Klicken Sie im Dialogfeld "Produktserver deaktivieren" auf "Deaktivieren".
In einer Meldung wird der Erfolg oder Misserfolg der Aktion angezeigt. In einigen Szenarien reagiert das Produkt möglicherweise nicht, sodass Protection Center das Produkt nicht wie gewöhnlich deaktivieren kann.
- 5 Klicken Sie bei Bedarf auf "Deaktivieren erzwingen".
- 6 Klicken Sie auf "Schließen".
Der deaktivierte Produkthost wird von der Registerkarte "Aktivierte unterstützte Produkte" entfernt und der Registerkarte "Verfügbare unterstützte Produkte" hinzugefügt.

Nicht verbundenes Produkt erneut aktivieren

Wenn Netzwerkprobleme in Ihrer Umgebung die Verbindung zwischen Protection Center und einem integrierten Produkt stören, ist das Produkt möglicherweise nicht mehr verbunden. Nicht verbundene Produkte unterbrechen die Datenzufuhr und die Übermittlung von Benachrichtigungen an Protection Center. Außerdem können sie nicht mehr über Protection Center verwaltet werden. Da das Produkt aber immer noch in Protection Center aktiviert ist, werden keine Daten verworfen. Wenn ein Produkt nicht mehr verbunden ist, müssen Sie den Verbindungsfehler beheben und das Produkt dann erneut aktivieren.

Siehe ["Info zu unterstützten Produkten"](#) auf Seite 29.

Siehe ["Integrieren unterstützter Produkte"](#) auf Seite 30.

Siehe ["Aktivieren eines unterstützten Produkts"](#) auf Seite 37.

So aktivieren Sie ein nicht verbundenes Produkt erneut

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Unterstützte Produkte".
- 2 Wählen Sie auf der Produktverwaltungsseite auf der Registerkarte "Aktivierte unterstützte Produkte" das Produkt, das Sie erneut aktivieren möchten.
- 3 Klicken Sie am rechten Ende des Produktbereichs auf "Verbindung: Fehler".
- 4 Lesen Sie die Fehlerdetails im Dialogfeld "Fehler bei der Verbindung" durch und führen Sie die zur Behebung notwendigen Schritte durch.
- 5 Klicken Sie auf "Neu aktivieren".

- 6** Geben Sie im Dialogfeld "Produkt erneut aktivieren" Sie die entsprechenden Einstellungen an.

Siehe "[Erforderliche unterstützte Produkthost-Einstellungen](#)" auf Seite 33.

- 7** Klicken Sie auf "Aktivieren".

- 8** Klicken Sie auf "OK".

Integrieren von Mail Security in Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Info zur Integration von Mail Security mit Protection Center](#)
- [Integrieren von Mail Security in Protection Center](#)
- [Aktivieren von Mail Security](#)
- [Installieren des Mail Security-Plugins auf Mail Security-Servern](#)
- [Installieren des Mail Security-Plugins unter Verwendung der Push-Methode](#)
- [Installieren des Mail Security-Plugins unter Verwendung der Pull-Methode](#)
- [Überwachen des Status von Mail Security-Vorgängen](#)
- [Info zu den Vorgangsstatusinformationen](#)
- [Upgrades des Mail Security-Plugins auf integrierten Mail Security-Servern](#)
- [Deinstallieren des Mail Security-Plugins von einem Mail Security-Server](#)

Info zur Integration von Mail Security mit Protection Center

Sie können Symantec Mail Security für Microsoft Exchange (Mail Security) mit Protection Center integrieren. Die Integration von Mail Security unterscheidet sich von der Integration anderer unterstützter Produkte in Protection Center.

Siehe ["Integrieren unterstützter Produkte"](#) auf Seite 30.

Um die Integration zahlreicher Server zu vereinfachen, stellt Protection Center alle Mail Security-Server in Ihrer Organisation als ein einziges Mail Security-Produkt dar.

Wenn Sie Mail Security mit Protection Center integrieren, müssen Sie die Mail Security-Hosts angeben, von denen Daten gesammelt werden sollen. Protection Center installiert auf jedem Mail Security-Host einen Management Agent und das Mail Security-Plugin.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Der repräsentative Mail Security-Server ermöglicht es, alle integrierten Mail Security-Server in Protection Center gemeinsam, d. h. als zusammengehörige Einheit zu verwalten. Wenn Sie Mail Security in Protection Center aktivieren, ermöglichen Sie die Integration beliebig vieler Mail Security-Server in Protection Center. Sie können die entsprechenden Mail Security-Server dann auswählen und das Mail Security-Plugin installieren, um die Integration abzuschließen. Alle integrierten Mail Security-Server-Instanzen werden über den repräsentativen Mail Security-Server mit Protection Center verbunden.

Protection Center sammelt Daten von allen integrierten Mail Security-Servern und stellt die Daten in den entsprechenden Berichten zur Verfügung. Auf der Registerkarte "Berichte" werden einige für Mail Security spezifische Berichte hinzugefügt. Diese Berichte enthalten ausführliche Informationen über den Status Ihrer E-Mail-Sicherheit. Einige Standardberichte wie zum Beispiel der Bericht "Malware-Zusammenfassung", enthalten eine Kombination aus Mail Security-Daten und Daten aus anderen Produkten.

Siehe ["Info zu speziellen Berichten für Mail Security"](#) auf Seite 144.

Siehe ["Anzeigen eines Berichts"](#) auf Seite 136.

Wenn Sie Mail Security in Protection Center deaktivieren, wird die Verbindung zu allen integrierten Mail Security-Servern sofort getrennt. Das Mail Security-Plugin wird automatisch von jedem Mail Security-Host deinstalliert. Wenn Sie Mail Security wieder aktivieren, müssen Sie das Mail Security-Plugin auf jedem Mail Security-Host neu installieren, den Sie mit Protection Center integrieren möchten.

Integrieren von Mail Security in Protection Center

Die Integration von Mail Security mit Protection Center unterscheidet sich von der Integration anderer Symantec-Produkte.

Siehe ["Info zur Integration von Mail Security mit Protection Center"](#) auf Seite 41.

Tabelle 5-1 Vorgang für die Integration von Mail-Sicherheit mit Protection Center

Schritt	Aktion	Beschreibung
Schritt 1	Aktivieren Sie das Mail Security-Produkt in Protection Center.	Sie können das virtuelle Mail Security-Produkt in Protection Center aktivieren. Durch Aktivieren dieses virtuellen Produkts werden alle Mail Security-Server in Ihrer Umgebung mit Protection Center integriert. Siehe "Aktivieren von Mail Security" auf Seite 44.
Schritt 2	Installieren Sie das Mail Security-Plugin auf Ihren Mail Security-Servern.	Sie müssen das Mail Security-Plugin auf jedem Mail Security-Server installieren, den Sie mit Protection Center integrieren möchten. Für die Installation des Mail Security-Plugins können Sie die manuelle Push-Methode oder die manuelle Pull-Methode verwenden. Siehe "Installieren des Mail Security-Plugins auf Mail Security-Servern" auf Seite 45. Siehe "Installieren des Mail Security-Plugins unter Verwendung der Push-Methode" auf Seite 46. Siehe "Installieren des Mail Security-Plugins unter Verwendung der Pull-Methode" auf Seite 47.
Schritt 3	Überwachen Sie den Fortschritt der Integration.	Sie können den Fortschritt der Installation des Mail Security-Plugins auf Ihren Mail Security-Servern überwachen und alle auftretenden Probleme sofort identifizieren. Ein Mail Security-Server gilt als integriert, wenn das Mail Security-Plugin ordnungsgemäß installiert ist und der Mail Security-Server beginnt, Daten an Protection Center zu senden. Siehe "Überwachen des Status von Mail Security-Vorgängen" auf Seite 49.
Schritt 4	Führen Sie nach Bedarf Upgrades für das Mail Security-Plugin durch.	Sie können auf allen verbundenen Hosts manuell Upgrades für das Mail Security-Plugin durchführen, wenn eine neue Version verfügbar wird. Protection Center führt keine automatischen Upgrades für das Mail Security-Plugin durch. Siehe "Upgrades des Mail Security-Plugins auf integrierten Mail Security-Servern" auf Seite 51.

Schritt	Aktion	Beschreibung
Schritt 5	(Optional) Deinstallieren Sie das Mail Security-Plugin manuell.	Sie können das Mail Security-Plugin von allen Mail Security-Servern, die nicht mehr mit Protection Center integriert sein sollen, manuell deinstallieren. Sie müssen das Mail Security-Plugin auch in den folgenden Szenarien manuell deinstallieren: ■ Das Mail Security-Plugin wurde per Push-Installation auf dem falschen Endgerät installiert. ■ Sie möchten Mail Security auf einen anderen Server migrieren. Siehe "Deinstallieren des Mail Security-Plugins von einem Mail Security-Server" auf Seite 52.

Aktivieren von Mail Security

Alle Mail Security-Server in Ihrer Organisation werden durch ein einziges Mail Security-Produkt in Protection Center dargestellt. Dieses repräsentative Mail Security-Produkt ist ein virtueller Mail Security-Server innerhalb von Protection Center. Das repräsentative Mail Security-Produkt ermöglicht es, alle integrierten Mail Security-Server in Protection Center gemeinsam, d. h. als zusammengehörige Einheit zu verwalten.

Siehe ["Info zur Integration von Mail Security mit Protection Center"](#) auf Seite 41.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Wenn Sie Mail Security in Protection Center aktivieren, ermöglichen Sie die Integration beliebig vieler Mail Security-Server in Protection Center. Sie können die entsprechenden Mail Security-Server dann auswählen und das Mail Security-Plugin installieren, um die Integration abzuschließen. Alle integrierten Mail Security-Server-Instanzen werden über den repräsentativen Mail Security-Server mit Protection Center verbunden.

So aktivieren Sie Mail Security

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Unterstützte Produkte".
- 2 Auf der Produktverwaltungsseite klicken Sie auf die Registerkarte "Verfügbare unterstützte Produkte".
- 3 Klicken Sie auf der Leiste "Symantec Mail Security für MS Exchange" auf "Unterstütztes Produkt aktivieren".
- 4 Klicken Sie in der erweiterten Leiste "Symantec Mail Security für MS Exchange" auf "Aktivieren".

Installieren des Mail Security-Plugins auf Mail Security-Servern

Sie müssen das Mail Security-Plugin auf jedem Mail Security-Server installieren, den Sie mit Protection Center integrieren möchten. Für die Installation des Mail Security-Plugins können Sie die manuelle Push-Methode oder die manuelle Pull-Methode verwenden. Symantec empfiehlt, dass Sie das Mail Security-Plugin mithilfe der manuellen Push-Methode auf den ausgewählten Servern installieren. Wenn Sie das Mail Security-Plugin jedoch auf einem Remote-Server installieren müssen, der nur begrenzten Netzwerkzugriff hat oder sich hinter einer Firewall befindet, müssen Sie möglicherweise eine manuelle Pull-Installation durchführen.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Tabelle 5-2 Methoden zum Installieren des Mail Security-Plugins

Methode	Beschreibung
Push-Installation	Die Push-Installation wird von Protection Center initiiert und das Mail Security-Plugin wird sofort installiert. Sie können das Mail Security-Plugin auf beliebig vielen Mail Security-Servern im selben Push-Vorgang installieren. Siehe "Installieren des Mail Security-Plugins unter Verwendung der Push-Methode" auf Seite 46.
Pull-Installation	Die Pull-Installation wird vom Endgerät initiiert, auf dem das Mail Security-Plugin installiert werden soll. Mit diesem Vorgang können Sie Firewalls und Zugriffsbeschränkungen im Netzwerk umgehen, die Push-Installationen auf Remote-Computern unter Umständen verhindern. Siehe "Installieren des Mail Security-Plugins unter Verwendung der Pull-Methode" auf Seite 47.

Warnung: Damit Sie die Push-Installationsmethode verwenden können, muss Protection Center in DNS registriert sein. Wenn Protection Center nicht registriert ist, müssen Sie die Pull-Installationsmethode verwenden. Sie müssen außerdem der Datei `hosts` auf jedem Mail Security-Server die IP-Adresse und den Hostnamen von Protection Center hinzufügen, bevor Sie den Installationsprozess beginnen.

Wenn Sie das Mail Security-Plugin auf einem Server installieren, wird automatisch auch der Symantec Management-Agent installiert. Der Symantec Management-Agent ist die Software, die die Kommunikation zwischen Protection Center und dem Mail Security-Server ermöglicht. Protection Center und der

Symantec Management-Agent installieren gemeinsam das Mail Security-Plugin und integrieren den Mail Security-Server mit Protection Center.

Der Installationsprozess dauert gewöhnlich einige Minuten. Der Symantec Management-Agent wird zuerst verteilt und löst eine Richtlinie in Protection Center aus, um das Mail Security-Plugin zu verteilen. Wenn die Installation des Plugins abgeschlossen ist, wird der Mail Security-Server mit dem virtuellen Server in Protection Center verbunden.

Sie können den Fortschritt der Installation des Mail Security-Plugins auf Ihren Mail Security-Servern überwachen und alle auftretenden Probleme identifizieren. Mögliche Gründe für ein Fehlschlagen der Installation sind: die Serveradresse war nicht auflösbar, die Windows-Admin\$-Freigabe war nicht aktiviert oder falsche Administrator-Identifikationsdaten wurden angegeben.

Installieren des Mail Security-Plugins unter Verwendung der Push-Methode

Sie können das Mail Security-Plugin auf mehreren Mail Security-Servern im selben Push-Vorgang installieren. Jedes angesteuerte Endgerät muss über ein 64-Bit-Betriebssystem verfügen und Mail Security muss darauf installiert sein. Die Windows Admin\$-Freigabe muss aktiviert sein. Sie müssen außerdem einen Satz Administrator-Identifikationsdaten angeben, die auf allen Zielcomputern gültig sind. Sie müssen außerdem der Datei `hosts` auf jedem Mail Security-Server die IP-Adresse und den Hostnamen von Protection Center hinzufügen, bevor Sie den Installationsprozess beginnen.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Siehe ["Installieren des Mail Security-Plugins auf Mail Security-Servern"](#) auf Seite 45.

Warnung: Damit Sie die Push-Installationsmethode verwenden können, muss Protection Center in DNS registriert sein. Wenn Protection Center nicht registriert ist, müssen Sie die Pull-Installationsmethode verwenden.

Wenn Sie versuchen, das Mail Security-Plugin auf einem 32-Bit-Computer oder auf einem Computer zu installieren, auf dem Mail Security nicht installiert ist, schlägt der Installationsprozess fehl. Auf 32-Bit-Computern löst das Fehlschlagen der Installation eine Deinstallationsrichtlinie aus, mit der der Symantec Management-Agent entfernt wird. Auf 64-Bit-Computern wird der Symantec Management-Agent jedoch nicht entfernt, wenn die Installation des Mail Security-Plugins fehlschlägt. Der Symantec Management-Agent wird auf dem

Computer beibehalten und kann dazu verwendet werden, die Ursachen für das Fehlschlagen zu beseitigen.

So installieren Sie das Mail Security-Plugin auf Mail Security-Servern

- 1 Klicken Sie in Protection Center in der Produktauswahl auf den nach unten zeigenden Pfeil.

Das Produktauswahlmenü befindet sich links neben dem Menü "Startseite" und zeigt den Namen des momentan ausgewählten Produkts an. Wenn Sie auf das Produktauswahlmenü klicken, wird eine Dropdown-Liste mit aktivierten Produkten angezeigt.

- 2 Klicken Sie auf "Symantec Mail Security für MS Exchange > Lokales SPC".
- 3 Klicken Sie in der Ansicht "Symantec Mail Security für MS Exchange" auf der Registerkarte "Konfiguration" auf "Windows-Installation".
- 4 Geben Sie im Dialogfeld "Windows-Installation" im Feld "Zielrechner" die Mail Security-Server an, die Sie mit Protection Center integrieren möchten.

Geben Sie manuell den Hostnamen oder die IP-Adresse jedes Mail Security-Servers ein, wobei Sie die einzelnen Einträge durch Kommas trennen. Sie können Hostnamen und IP-Adressen in der Liste mischen.

- 5 Geben Sie den Benutzernamen und das Kennwort für ein Administratorkonto auf den angesteuerten Mail Security-Servern an.

Die gleichen Identifikationsdaten werden für alle angesteuerten Mail Security-Server verwendet. Sie können das Mail Security-Plugin an eine Gruppe von Servern verteilen, die die gleichen Identifikationsdaten haben, z. B. die Server in einer einzelnen Domäne.

- 6 Klicken Sie auf "OK".
- 7 Wenn Sie die Installation des Mail Security-Plugins überwachen möchten, klicken Sie auf "Vorgangsstatus".

Die Installation des Mail Security-Plugins dauert gewöhnlich einige Minuten. Im Dialogfeld "Vorgangsstatus" können Sie den aktuellen Status des Mail Security-Plugins auf den angesteuerten Mail Security-Servern anzeigen.

Siehe ["Überwachen des Status von Mail Security-Vorgängen"](#) auf Seite 49.

Installieren des Mail Security-Plugins unter Verwendung der Pull-Methode

Auf Mail Security-Servern, die begrenzten Netzwerkzugriff haben oder sich hinter einer Firewall befinden, müssen Sie das Mail Security-Plugin möglicherweise

installieren. Um diese Beschränkung zu umgehen, können Sie die Pull-Methode zur Installation des Mail Security-Plugins auf den einzelnen Computern verwenden. Sie müssen sich auf jedem Computer einloggen und über eine URL auf Protection Center zugreifen, um den Installationsprozess für das Mail Security-Plugin zu starten. Der Installationsprozess läuft normalerweise automatisch ab, ohne weiteren Benutzereingriff zu benötigen.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Siehe ["Installieren des Mail Security-Plugins auf Mail Security-Servern"](#) auf Seite 45.

Die Pull-URL, die in der Protection Center-Schnittstelle bereitgestellt wird, verwendet die gleiche Schreibweise, die Sie auch für den Zugriff auf Protection Center verwendet haben. Die Verbindung zwischen Protection Center und dem Mail Security-Server ist zuverlässiger, wenn der DNS-Name von Protection Center verwendet wird. Aus diesem Grund sollten Sie auf Protection Center unter Verwendung seines DNS-Namens anstelle seiner IP-Adresse zugreifen, um die Pull-URL abzurufen. Sie müssen außerdem der Datei `hosts` auf jedem Mail Security-Server die IP-Adresse und den Hostnamen von Protection Center hinzufügen, bevor Sie den Installationsprozess beginnen.

So rufen Sie die URL für die Pull-Installation ab

- 1** Greifen Sie auf Protection Center zu, wobei Sie dessen DNS-Namen verwenden.
- 2** Klicken Sie in Protection Center in der Produktauswahl auf den nach unten zeigenden Pfeil.
- 3** Klicken Sie auf "Symantec Mail Security für MS Exchange > Lokales SPC".
- 4** Notieren Sie die in der Ansicht "Symantec Mail Security für MS Exchange" auf der Registerkarte "Konfiguration" unter "Pull-Installation (manuell)" angegebene URL.

So installieren Sie das Mail Security-Plugin unter Verwendung der Pull-Methode

- 1 Loggen Sie sich beim entsprechenden Mail Security-Server als Administrator ein.

Sie können sich mithilfe einer Remote-Zugriffsanwendung wie z.B. pcAnywhere remote einloggen oder einen Benutzer auffordern, sich mit einem entsprechenden Konto einzuloggen.

- 2 Auf dem Mail Security-Server öffnen Sie einen Browser und navigieren Sie zu der URL, die Sie im vorherigen Schritt notiert haben.

Wenn die URL eine IP-Adresse verwendet, werden Sie in einer Warnmeldung darauf hingewiesen, dass die Verbindung zwischen Protection Center und dem Mail Security-Server möglicherweise gestört werden könnte. Die Verbindung ist zuverlässiger, wenn stattdessen der DNS-Name von Protection Center DNS verwendet wird.

- 3 Auf der Seite "Agent-Installation" aktivieren Sie "Symantec Management-Agent installieren und folgendes Plugin auf diesem Rechner ablegen:" SMSMSE Agent Plug-in

- 4 Klicken Sie auf "Starten".

Wenn Sie Microsoft Internet Explorer verwendet haben, weist eine Meldung darauf hin, dass der Vorgang abgeschlossen ist. Der Installationsprozess für das Mail Security-Plugin läuft automatisch ab.

Der Installationsprozess dauert gewöhnlich einige Minuten. Im Dialogfeld "Vorgangstatus" können Sie den aktuellen Status des Symantec Management-Agent und des Mail Security-Plugins auf den angesteuerten Mail Security-Servern anzeigen.

Siehe "[Überwachen des Status von Mail Security-Vorgängen](#)" auf Seite 49.

Wenn Sie Mozilla Firefox verwendet haben, müssen Sie die Anweisungen auf der Seite "Agent-Installation" befolgen, um das Paket herunterzuladen und zu installieren.

Überwachen des Status von Mail Security-Vorgängen

Sie können den Status von Installationen, Aktualisierungen und Deinstallationen des Mail Security-Plugins überwachen.

Siehe "[Integrieren von Mail Security in Protection Center](#)" auf Seite 42.

So überwachen Sie den Status von Mail Security-Vorgängen

- 1

Klicken Sie in Protection Center in der Produktauswahl auf den nach unten zeigenden Pfeil.
- 2

Klicken Sie auf "Symantec Mail Security für MS Exchange > Lokales SPC".
- 3

Klicken Sie in der Ansicht "Symantec Mail Security für MS Exchange" auf der Registerkarte "Konfiguration" auf "Vorgangsstatus".
- 4

Im Dialogfeld "Vorgangsstatus" können Status von Installationen, Aktualisierungen und Deinstallationen des Mail Security-Plugins überwachen.
Siehe ["Info zu den Vorgangsstatusinformationen"](#) auf Seite 50.
- 5

Um sicherzustellen, dass das Dialogfeld "Vorgangsstatus" die neuesten Informationen enthält, klicken Sie auf "Aktualisieren".

Die Back-End-Vorgänge können einige Minuten dauern und das Dialogfeld "Vorgangsstatus" wird nicht automatisch aktualisiert.
- 6

Klicken Sie auf "OK", um das Dialogfeld "Vorgangsstatus" zu schließen.

Info zu den Vorgangsstatusinformationen

Das Dialogfeld "Vorgangsstatus" zeigt die Echtzeitansicht von Mail Security-Vorgängen während der letzten sieben Tage an. Mithilfe dieser Funktion können Sie den aktuellen Status des Symantec Management-Agent und des Mail Security-Plugins anzeigen, während diese auf den Mail Security-Servern installiert werden.

Siehe ["Überwachen des Status von Mail Security-Vorgängen"](#) auf Seite 49.

Tabelle 5-3 Im Dialogfeld "Vorgangsstatus" angezeigte Informationen

Element	Beschreibung
Angeforderte Zeit	Zeigt die Startzeit des Vorgangs an.
Name	Zeigt den Namen des Mail Security-Servers an.
IP-Adresse	Zeigt die IP-Adresse des Mail Security-Servers an.
Vorgang	Zeigt den Vorgang an, der angefordert wurde, ausgeführt wird oder abgeschlossen wurde.

Element	Beschreibung
Status	Zeigt den aktuellen Status des Vorgangs an. Für die Installation des Plugins werden normalerweise die folgenden Informationen angezeigt: ■ Eine Push- oder Pull-Installation wurde initiiert, steht aus oder wird durchgeführt. ■ Der Symantec Management-Agent wird installiert. ■ Der Symantec Management-Agent hat Inventar an Protection Center gesendet. ■ Eine Richtlinienaktualisierung ist angefordert worden. ■ Das Mail Security-Plugin wird installiert.
Detail	Zeigt Informationen zum Status des Vorgangs an.

Upgrades des Mail Security-Plugins auf integrierten Mail Security-Servern

Protection Center führt keine automatischen Upgrades des Mail Security-Plugins auf den standortfernen Mail Security-Servern durch. Wenn eine neue Version des Mail Security-Plugins verfügbar wird, müssen Sie die Upgrades manuell durchführen.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

So führen Sie Upgrades des Mail Security-Plugins auf integrierten Mail Security-Servern durch

- 1 Klicken Sie in Protection Center in der Produktauswahl auf den nach unten zeigenden Pfeil.
- 2 Klicken Sie auf "Symantec Mail Security für MS Exchange > Lokales SPC".
- 3 Klicken Sie in der Ansicht "Symantec Mail Security für MS Exchange" auf der Registerkarte "Konfiguration" auf "Plugin aktualisieren".
- 4 Klicken Sie im Dialogfeld "Plugin aktualisieren" auf "Ressourcen auswählen".
- 5 Wählen Sie im Dialogfeld "Ziele auswählen" die Mail Security-Server, für die Sie das Mail Security-Plugin aktualisieren möchten, und klicken Sie dann auf "OK".
- 6 Prüfen Sie im Dialogfeld "Plugin aktualisieren", ob die Liste der Server richtig ist, und klicken Sie dann auf "Plugin aktualisieren".

- 7 Klicken Sie auf "Schließen".
- 8 Wenn Sie die Aktualisierung des Mail Security-Plugins überwachen möchten, klicken Sie auf "Vorgangstatus".

Im Dialogfeld "Vorgangstatus" können Sie den aktuellen Status des Mail Security-Plugins auf Ihren Mail Security-Servern anzeigen.

Siehe ["Überwachen des Status von Mail Security-Vorgängen"](#) auf Seite 49.

Deinstallieren des Mail Security-Plugins von einem Mail Security-Server

Sie können das Mail Security-Plugin erforderlichenfalls manuell von den angegebenen Servern deinstallieren. Wenn Sie das Mail Security-Plugin von einem Endgerät deinstallieren, wird der Symantec Management-Agent automatisch entfernt.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Wenn Sie die Instanz des Mail Security-Produkts in Protection Center deaktivieren, wird das Mail Security-Plugin automatisch von jedem integrierten Mail Security-Server deinstalliert.

Sie müssen das Mail Security-Plugin in den folgenden Fällen eventuell manuell deinstallieren:

- Das Mail Security-Plugin wurde per Push-Installation auf dem falschen Endgerät installiert.
- Sie müssen Mail Security auf einen anderen Server migrieren.
- Der Mail Security-Server soll keine Daten mehr an Protection Center senden.

So deinstallieren Sie das Mail Security-Plugin von einem Mail Security-Server

- 1 Klicken Sie in Protection Center in der Produktauswahl auf den nach unten zeigenden Pfeil.
- 2 Klicken Sie auf "Symantec Mail Security für MS Exchange > Lokales SPC".
- 3 Klicken Sie in der Ansicht "Symantec Mail Security für MS Exchange" auf der Registerkarte "Konfiguration" auf "Plugin deinstallieren".
- 4 Im Dialogfeld "Plugin deinstallieren" klicken Sie auf "Ressourcen auswählen".
- 5 Im Dialogfeld "Ziele auswählen" wählen Sie die Endgeräte, von denen Sie Plugins deinstallieren möchten, und klicken Sie dann auf "OK".

- 6 Überprüfen Sie im Dialogfeld "Plugin deinstallieren" unter "Name", ob die Liste von Computern richtig ist, und klicken Sie dann auf "Plugin deinstallieren".
- 7 Klicken Sie auf "Schließen".
- 8 Wenn Sie die Deinstallation des Mail Security-Plugins überwachen möchten, klicken Sie auf "Vorgangstatus".

Im Dialogfeld "Vorgangstatus" können Sie den aktuellen Status des Symantec Management-Agent und des Mail Security-Plugins auf den angesteuerten Endgeräten anzeigen.

Siehe ["Überwachen des Status von Mail Security-Vorgängen"](#) auf Seite 49.

Verwalten von Protection Center-Benutzerkonten

In diesem Kapitel werden folgende Themen behandelt:

- [Über Protection Center-Benutzerkonten](#)
- [Info zum SPC_Admin-Konto](#)
- [Einrichten von Protection Center-Benutzerkonten](#)
- [Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung](#)
- [Optionen für die Protection Center-Benutzerkontoverwaltung](#)
- [Erstellen von Protection Center-Benutzerkonten](#)
- [Ändern eines Protection Center-Benutzerkontos](#)
- [Authentifizierungstypen für Protection Center-Benutzerkonten](#)
- [Benutzerauthentifizierungseinstellungen für Protection Center \(lokal\)](#)
- [Active Directory- und LDAP-Authentifizierungseinstellungen](#)
- [Protection Center-Benutzerkontoberechtigungseinstellungen](#)
- [Protection Center-Benutzerkontoberechtigungen](#)
- [Unterstützte Produktzugriffsberechtigungseinstellungen](#)
- [Löschen eines Protection Center-Benutzerkontos](#)

Über Protection Center-Benutzerkonten

Jeder Protection Center-Benutzer besitzt ein eigenes Benutzerkonto. Mit dem Protection Center-Benutzerkonto hat der Benutzer Zugriff auf spezifische Protection Center-Funktionen. Der Benutzer kann über das Protection Center-Benutzerkonto auch auf bestimmte unterstützte Produkte und die Produktdaten zugreifen. Sie können Protection Center-Benutzerkonten erstellen, ändern, deaktivieren und löschen.

Siehe ["Einrichten von Protection Center-Benutzerkonten"](#) auf Seite 57.

Über das vordefinierte Protection Center-Administratorkonto (SPC_Admin) besteht uneingeschränkter Zugriff auf alle Funktionen von Protection Center. Nach erstmaliger Bereitstellung von Protection Center müssen Sie sich zum Erstellen weiterer Protection Center-Benutzerkonten in das SPC_Admin-Konto einloggen.

Siehe ["Info zum SPC_Admin-Konto"](#) auf Seite 57.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Siehe ["Löschen eines Protection Center-Benutzerkontos"](#) auf Seite 76.

Tabelle 6-1 Protection Center-Benutzerkontofunktionen

Parameter	Beschreibung
Eindeutiger Benutzername	Der gleiche Benutzername kann nicht für zwei Benutzerkonten verwendet werden, selbst wenn die Authentifizierungsmethoden beider Benutzerkonten unterschiedlich sind.
Authentifizierungstyp	Protection Center kann Benutzer über lokale Konten, Microsoft Active Directory oder LDAP authentifizieren. Siehe "Authentifizierungstypen für Protection Center-Benutzerkonten" auf Seite 67.
Funktionsberechtigungen	Dem vordefinierten Administratorkonto, SPC_Admin, sind alle verfügbaren Berechtigungen zugewiesen. Sie können jedoch allen weiteren Benutzerkonten einen reduzierten Satz an Berechtigungen zuweisen. Siehe "Protection Center-Benutzerkontoberechtigungseinstellungen" auf Seite 70.
Produkte	Benutzern können die Rechte zugewiesen werden, auf die in Protection Center integrierten Produkte zuzugreifen. Hat ein Benutzer Zugriff auf ein Produkt, kann er Daten aus diesem Produkt in Protection Center-Berichten anzeigen. Hat ein Benutzer keinen Zugriff auf ein Produkt, werden die Daten von diesem Produkt nicht in Protection Center-Berichten einbezogen, die der Benutzer anzeigt. Siehe "Unterstützte Produktzugriffsberechtigungseinstellungen" auf Seite 75.

Info zum SPC_Admin-Konto

Über das vordefinierte Protection Center-Administratorkonto (SPC_Admin) besteht uneingeschränkter Zugriff auf alle Funktionen von Protection Center. Nach der ersten Bereitstellung von Protection Center müssen Sie das SPC_Admin-Konto verwenden, um auf andere Protection Center-Benutzerkonten zuzugreifen und diese zu erstellen.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Das erste Kennwort für das SPC_Admin-Konto wird bei der Erstellung der Protection Center-Appliance festgelegt. Das SPC_Admin-Konto kann weder deaktiviert noch aus Protection Center entfernt werden. Sie können das Kennwort sowohl über die Ansicht "Protection Center" als auch über die Protection Center-Systemsteuerung ändern.

Siehe ["Zugreifen auf die Protection Center-Systemsteuerung"](#) auf Seite 107.

Siehe ["Ändern des Kennworts für das SPC_Admin-Konto"](#) auf Seite 108.

Einrichten von Protection Center-Benutzerkonten

Jeder Protection Center-Benutzer benötigt ein eigenes Benutzerkonto. Nach erstmaliger Bereitstellung von Protection Center müssen Sie sich zum Erstellen weiterer Protection Center-Benutzerkonten in das SPC_Admin-Konto einloggen. Sie können Protection Center-Benutzerkonten erstellen, ändern, deaktivieren und löschen.

Tabelle 6-2 Prozess für das Einrichten von Protection Center-Benutzerkonten

Schritt	Aktion	Beschreibung
Schritt 1	Planen Sie Ihre Protection Center-Benutzerkonten.	Möglicherweise haben Sie bereits Microsoft Active Directory- oder LDAP-Benutzerkonten für Ihr Netzwerk eingerichtet. Sie können diese vorhandenen Konten als Grundlage für entsprechende Protection Center-Benutzerkonten verwenden. Microsoft Active Directory oder LDAP authentifiziert die Benutzeridentifikationsdaten, sobald der Benutzer sich bei Protection Center einloggt. Alternativ können Sie neue Konten in Protection Center erstellen und die Benutzeridentifikationsdaten von Protection Center authentifizieren lassen. Siehe "Über Protection Center-Benutzerkonten" auf Seite 56. Siehe "Optionen für die Protection Center-Benutzerkontoverwaltung" auf Seite 63.

Schritt	Aktion	Beschreibung
Schritt 2	Geben Sie einen Active Directory oder LDAP-Server an.	Falls Sie bestehende Microsoft Active Directory- oder LDAP-Benutzerkonten verwenden möchten, müssen Sie den entsprechenden Active Directory- oder LDAP-Server angeben. Siehe "Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung" auf Seite 58.
Schritt 3	Erstellen Sie jedes Protection Center-Benutzerkonto.	Sie müssen die Authentifizierungsmethode für das Konto auswählen und anschließend die Benutzerdetails angeben oder das entsprechende Active Directory oder LDAP-Konto auswählen. Siehe "Erstellen von Protection Center-Benutzerkonten" auf Seite 64. Siehe "Authentifizierungstypen für Protection Center-Benutzerkonten" auf Seite 67. Sie müssen dem Benutzerkonto die entsprechenden Berechtigungen zuweisen. Siehe "Protection Center-Benutzerkontoberechtigungseinstellungen" auf Seite 70. Sie müssen die unterstützten Produkte auswählen, auf die das Benutzerkonto über Protection Center Zugriff hat. Siehe "Unterstützte Produktzugriffsberechtigungseinstellungen" auf Seite 75.
Schritt 4	Ändern Sie und verwalten Sie Benutzerkonten nach Bedarf.	Sie können ein Protection Center-Benutzerkonto jederzeit ändern. Verändern Sie allerdings die Authentifizierungsmethode, wird ein neues Benutzerkonto erstellt, das das ursprüngliche Konto ersetzt. Siehe "Ändern eines Protection Center-Benutzerkontos" auf Seite 66. Siehe "Löschen eines Protection Center-Benutzerkontos" auf Seite 76.

Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung

Sie können die in Ihrem Netzwerk eingerichteten Microsoft Active Directory- oder LDAP-Benutzerkonten verwenden, um entsprechende Protection Center-Benutzerkonten zu authentifizieren. Sie müssen die entsprechenden Active Directory- oder LDAP-Server angeben, um Microsoft Active Directory- oder LDAP-Benutzerkonten in Protection Center zu verwenden. Geben Sie den Servernamen und die entsprechenden Identifikationsdaten an, um auf den Server zuzugreifen. Sie müssen auch den entsprechenden Basis-Distinguished Namen (Basis-DN) und den Filter für die Benutzersuche angeben.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Einrichten von Protection Center-Benutzerkonten"](#) auf Seite 57.

Siehe ["Authentifizierungstypen für Protection Center-Benutzerkonten"](#) auf Seite 67.

Siehe ["Active Directory- und LDAP-Authentifizierungseinstellungen"](#) auf Seite 69.

Wenn Sie ein Protection Center-Benutzerkonto erstellen, können Sie den Namen eines vorhandenen Active Directory- oder LDAP-Kontos angeben. Protection Center importiert die entsprechenden Kontodetails vom angegebenen Active Directory- oder LDAP-Server. Loggt sich ein Benutzer bei Protection Center ein, authentifiziert Active Directory oder LDAP die Benutzeridentifikationsdaten.

So verwenden Sie einen Active Directory- oder LDAP-Server zur Benutzerkontoauthentifizierung

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Active Directory und LDAP".
- 2 Geben Sie auf der Active Directory- und LDAP-Servereinstellungsseite die entsprechenden Details an.

Siehe [""Active Directory und LDAP"-Servereinstellungen"](#) auf Seite 59.
- 3 Klicken Sie auf "LDAP-Einstellungen testen" oder "Änderungen speichern".

Protection Center überprüft, ob die Einstellungen richtig angegeben sind. Falls Einstellungen nicht überprüft werden können, wird eine entsprechende Fehlermeldung angezeigt. Wurden alle Einstellungen verifiziert, speichert Protection Center die Einstellungen.

"Active Directory und LDAP"-Servereinstellungen

Mit den "Active Directory und LDAP"-Servereinstellungsseite können Sie den "Active Directory oder LDAP"-Server angeben, um Protection Center-Benutzerkonten zu authentifizieren. Sie können die Abfrage "LDAP" auch angeben, die die Active Directory-Benutzer extrahiert, die Sie Protection Center hinzufügen möchten.

Siehe ["Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung"](#) auf Seite 58.

Tabelle 6-3 "Active Directory und LDAP"-Servereinstellungen

Element	Beschreibung
Hostname	Gibt den Server an, auf dem sich Microsoft Active Directory oder der Domänencontroller befindet. Sie können den Hostnamen oder die IP-Adresse eingeben.

Element	Beschreibung
Benutzername	Gibt den Benutzernamen eines Konten an, das Administratorrechte für den "Active Directory oder LDAP"-Server hat. Verwenden Sie die <i><Benutzernamen></i>syntax; verwenden Sie nicht die <i><Domäne-\Benutzernamen></i>syntax. Diese Einstellung ist für sichere Authentifizierung erforderlich. Sicheres Login zum Active Directory wird standardmäßig aktiviert, also sollten Sie Benutzer-Login-Informationen für den ersten Verbindungsversuch angeben.
Kennwort	Gibt das Kennwort des Administratorkontos an.
Authentication Type	Gibt die Methode, wie Protection Center den "Active Directory oder LDAP"-Server abfragt, wie folgt an: ■ Sicher Die Verbindungsanforderung sendet Informationen, die Sie konfiguriert haben. Protection Center stellt eine sichere Verbindung mit dem "Active Directory oder LDAP"-Server her. Sie müssen den entsprechenden Benutzernamen und das Kennwort angeben. ■ Anonym Die Verbindungsanforderung verwendet keine Identifikationsdaten.
"SSL verwenden"	Gibt an, dass Protection Center SSL für Kommunikation mit dem "Active Directory oder LDAP"-Server verwendet. Damit dies funktioniert, muss Ihr "Active Directory oder LDAP"-Server richtig konfiguriert werden um SSL zu verwenden.
Basis-DN	Gibt den Basis-Distinguished Name an: Die erste Ebene der "LDAP"-Verzeichnisstruktur.
Erstellen	Öffnet das Dialogfeld Basis Distinguished-Name erstellen, womit Sie den Basis-DN angeben können. Siehe "Angeben des Basis-DN" auf Seite 61.
Benutzersuchfilter	Gibt die Filtersuchzeichenfolge an, um die Benutzerinformationen zu extrahieren, die für Protection Center erforderlich sind.
Erstellen	Öffnet das Dialogfeld "Suchfilter erstellen", womit Sie die Filtersuchzeichenfolge angeben können. Siehe "Angeben des Filters für die Benutzersuche" auf Seite 62.

Element	Beschreibung
"LDAP-Einstellungen testen"	Testet die Einstellungen, um zu überprüfen, dass sie richtig angegeben wurden. Diese Option kopiert die "Änderungen speichern" -Funktion. Protection Center überprüft Folgendes: ■ Sie haben Zugriff auf den angegebene LDAP-Server. ■ Der angegebene Ordner "Basis-DN" existiert. ■ Die angegebene Benutzersuche-Filtersyntax ist richtig. Protection Center überprüft nicht, dass der Suchfilter alle Benutzer zurückgibt. Falls Einstellungen nicht überprüft werden können, wird eine entsprechende Fehlermeldung angezeigt. Wurden alle Einstellungen verifiziert, speichert Protection Center die Einstellungen.

Angeben des Basis-DN

Sie müssen den Basis-DN für die "Active Directory und LDAP"-Servereinstellungen angeben. Der Basis-DN ist die erste Ebene der "LDAP"-Verzeichnisstruktur. Abhängig davon, wie Active Directory in Ihrem Unternehmen eingerichtet ist, kann der Basis-DN ein oder mehrere Werte haben, um den Ort, in dem nach einem Benutzer gesucht wird, anzuzeigen.

Siehe ["Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung"](#) auf Seite 58.

Sie müssen jeden Basis-DN-Wert über einen **DC= Präfix**-Eintrag angeben und mehrere Werte durch Kommas trennen.

Ein Beispiel folgt:

CN=Users, DC=myDomain, DC=com

wo **Benutzer** der Name des Behälters ist, in dem sich die Benutzerkonten in der Verzeichnisstruktur befinden. Dieser Behälter befindet sich im Stamm von **myDomain.com** , der normalerweise die Zone oder Ihr Domänenname ist.

So geben Sie den Basis-DN an

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Active Directory und LDAP".
- 2 Klicken Sie auf der "Active Directory und LDAP"-Servereinstellungsseite neben "Basis-DN" auf Erstellen.

- 3 Klicken Sie im Dialogfeld "Basis Distinguished-Name erstellen" auf den zu verwendenden Ordner.

Das Feld "Ausgewählter DN" zeigt den ausgewählten Ordnernamen an.

- 4 Klicken Sie auf "OK".

Der angegebene Basis-DN wird zum Feld "Basis-DN" auf der "Active Directory und LDAP"-Servereinstellungsseite hinzugefügt.

Angeben des Filters für die Benutzersuche

Sie müssen den Filter für die Benutzersuche für die "Active Directory und LDAP"-Servereinstellungen angeben. Mit der Filtersuchzeichenfolge kann Protection Center die Benutzerinformationen, die vom LDAP-Server erforderlich sind, extrahieren.

Siehe ["Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung"](#) auf Seite 58.

Ein Beispiel für Suchfilter folgt:

(&(objectClass=user) ((anr=%s*) (uid=%s*)))

Wo:

- **objectClass=user**
Gibt den Typ des zu durchsuchenden Objekts an.
- **anr=**
Gibt vieldeutige Namensauflösung an.
- **uid=**
Gibt an, auch nach Benutzer-ID zu suchen.
- **%s***
Gibt teilweise Zeichenfolge sowie ganzen Namen an.

So geben Sie den Filter für die Benutzersuche an

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Active Directory und LDAP".
- 2 Klicken Sie auf der "Active Directory und LDAP"-Servereinstellungsseite neben "Filter für die Benutzersuche" auf Erstellen.

- 3 Im Dialogfeld "Suchfilter erstellen" im Feld "Suche nach Benutzer", geben Sie den Namen eines Benutzers ein, der auf dem LDAP-Server existiert.
 Wenn Sie mit dem Eingeben des Namens beginnen, wählen Sie den entsprechenden Benutzer aus der Liste. Wenn Sie einen Benutzer auswählen, wird eine Liste von Eigenschaften, die der LDAP-Server für den ausgewählten Benutzer speichert, angezeigt.
- 4 Wählen Sie die Objekt-Klassen und die Benutzereigenschaften aus, die Sie in Ihren Benutzersuchen einschließen möchten.
- 5 Das Feld "Filter für die Benutzersuche" zeigt die Syntax des entsprechenden Filters für die Benutzersuche an.
- 6 Klicken Sie auf "OK".
 Die angegebene Filterzeichenfolge für die Benutzersuche wird dem Feld "Filter für die Benutzersuche" auf der "Active Directory und LDAP"-Servereinstellungsseite hinzugefügt.

Optionen für die Protection Center-Benutzerkontoverwaltung

Die Protection Center-Benutzerverwaltungsseite zeigt eine Übersicht aller Protection Center-Benutzerkonten an. Sie können Protection Center-Benutzerkonten erstellen, ändern und löschen. Zur regelmäßigen Verwaltung von Protection Center-Benutzerkonten gehört u. U. das Zurücksetzen vergessener oder gefährdeter Kennwörter. Sie müssen möglicherweise auch die Benutzerkonten deaktivieren, die nicht mehr erforderlich sind.

Sie können die Liste von Benutzerkonten sortieren, indem Sie auf die Überschrift der Spalte klicken, die Sie sortieren möchten. Sie können auf ein Konto doppelklicken, um das Dialogfeld "Benutzerkonto bearbeiten" für dieses Benutzerkonto zu öffnen.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Einrichten von Protection Center-Benutzerkonten"](#) auf Seite 57.

Tabelle 6-4 Optionen für die Protection Center-Benutzerkontoverwaltung

Option	Beschreibung
Neu	Greift auf das Dialogfeld "Benutzerkonto erstellen" zu, sodass Sie ein Protection Center-Benutzerkonto erstellen können. Siehe "Erstellen von Protection Center-Benutzerkonten" auf Seite 64.

Option	Beschreibung
Bearbeiten	Greift auf das Dialogfeld "Benutzerkonto bearbeiten" zu, sodass Sie das ausgewählte Protection Center-Benutzerkonto ändern können. Siehe "Ändern eines Protection Center-Benutzerkontos" auf Seite 66.
Löschen	Greift auf das Dialogfeld "Benutzerkonto löschen" zu, sodass Sie ein Protection Center-Benutzerkonto löschen können. Siehe "Löschen eines Protection Center-Benutzerkontos" auf Seite 76.

Erstellen von Protection Center-Benutzerkonten

Sie müssen für jeden Protection Center-Benutzer ein Benutzerkonto erstellen. Mit dem Protection Center-Benutzerkonto hat der Benutzer Zugriff auf spezifische Protection Center-Funktionen. Der Benutzer kann über das Protection Center-Benutzerkonto auch auf bestimmte aktivierte Produkte und auf von diesen bereitgestellte Daten zugreifen.

Protection Center kann entweder Benutzerkonten selbst authentifizieren oder die Benutzeridentifikationsdaten mithilfe von Microsoft Active Directory oder LDAP authentifizieren. Indem Sie Microsoft Active Directory- oder LDAP-Authentifizierung für Protection Center-Benutzerkonten implementieren, können Sie für Protection Center-Benutzer auf Ihren normalen Domänenauthentifizierungsdienst zurückgreifen. Sie müssen die entsprechenden Active Directory- oder LDAP-Server angeben, um Microsoft Active Directory- oder LDAP-Benutzerkonten in Protection Center verwenden zu können.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Einrichten von Protection Center-Benutzerkonten"](#) auf Seite 57.

Siehe ["Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung"](#) auf Seite 58.

So erstellen Sie ein Protection Center-Benutzerkonto

1 In Protection Center haben Sie folgende Möglichkeiten:

So erstellen Sie ein Benutzerkonto im Rahmen des ersten Einrichtens	Klicken Sie im ersten Einstellungsdialogfeld unter "Benutzerkonten", auf "Konten erstellen".
So erstellen Sie ein Benutzerkonto über die Benutzerverwaltungsseite	Klicken Sie im Menü "Admin" auf "Benutzerverwaltung". Klicken Sie auf der Benutzerverwaltungsseite auf "Neu".

2 Klicken Sie im Dialogfeld "Benutzerkonten" oder im Dialogfeld "Benutzerkonto erstellen" auf die Authentifizierungsmethode, die Sie für das neue Protection Center-Benutzerkonto verwenden möchten:

Lokal authentifiziertes Konto	Erstellt ein lokales Benutzerkonto in Protection Center.
Authentifiziertes Active Directory- oder LDAP-Konto	Erstellt ein Benutzerkonto, das von Ihrem Active Directory- oder LDAP-Server authentifiziert wird.

Siehe ["Authentifizierungstypen für Protection Center-Benutzerkonten"](#) auf Seite 67.

3 Sie haben folgende Möglichkeiten:

Für ein lokales Konto	Geben Sie die lokalen Kontoinformationen an. Siehe "Benutzerauthentifizierungseinstellungen für Protection Center (lokal)" auf Seite 68.
Für ein Active Directory- oder LDAP-Konto	Geben Sie das zu verwendende Active Directory- bzw. LDAP-Konto an. Protection Center extrahiert die Kontodetails vom Active Directory- oder LDAP-Server. Siehe "Active Directory- und LDAP-Authentifizierungseinstellungen" auf Seite 69.

4 Geben Sie die Protection Center-Benutzerberechtigungen für das Konto an. Siehe ["Protection Center-Benutzerkontoberechtigungseinstellungen"](#) auf Seite 70.

- 5 Geben Sie auf die unterstützten Produkte an, auf die das Konto zugreifen kann.
Siehe "[Unterstützte Produktzugriffsberechtigungseinstellungen](#)" auf Seite 75.
- 6 Klicken Sie auf "Speichern".
- 7 Überprüfen und bestätigen Sie die Benutzerdetails.
- 8 (Optional) Wenn Sie den Benutzer benachrichtigen möchten, dass das neue Protection Center-Benutzerkonto verfügbar ist, klicken Sie auf "Benachrichtigung an diesen Benutzer senden".
Protection Center sendet eine E-Mail-Benachrichtigung an die in den Authentifizierungseinstellungen angegebene E-Mail-Adresse.
Beachten Sie, dass diese Option nur dann verfügbar ist, wenn ein E-Mail-Server für Protection Center konfiguriert ist und eine E-Mail-Adresse im neuen Benutzerkonto angegeben wurde.
Siehe "[E-Mail-Einstellungen](#)" auf Seite 97.
- 9 Klicken Sie auf "Fertig stellen".

Ändern eines Protection Center-Benutzerkontos

Sie können ein Protection Center-Benutzerkonto jederzeit ändern. Sie müssten möglicherweise ein Konto ändern, um dem Benutzer Zugriff auf ein neues aktiviertes Produkt zu geben, oder um die Protection Center-Benutzerberechtigungen zu ändern. Beachten Sie, dass beim Ändern der Authentifizierungsmethode ein neues Benutzerkonto erstellt wird, das das ursprüngliche Konto ersetzt.

Siehe "[Über Protection Center-Benutzerkonten](#)" auf Seite 56.

Siehe "[Einrichten von Protection Center-Benutzerkonten](#)" auf Seite 57.

Im Rahmen der regulären Verwaltung müssen Sie möglicherweise Kennwörter zurücksetzen, die vergessen wurden oder gefährdet sind. Außerdem müssen Sie möglicherweise auch Benutzerkonten deaktivieren, die nicht mehr benötigt werden.

Das vordefinierte Protection Center-Administratorkonto "SPC_Admin" kann nicht deaktiviert oder entfernt werden.

Siehe "[Info zum SPC_Admin-Konto](#)" auf Seite 57.

So ändern Sie ein Protection Center-Benutzerkonto

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Benutzerverwaltung".
- 2 Wählen Sie auf der Benutzerverwaltungsseite das Konto aus, das Sie ändern möchten, und klicken Sie anschließend auf "Bearbeiten".

Außerdem können Sie auf das ausgewählte Konto doppelklicken.

- 3 Im Dialogfeld "Protection Center-Benutzerkonto bearbeiten" auf der Registerkarte "Kontodetails und -berechtigungen" bearbeiten Sie die Einstellungen für das Protection Center-Benutzerkonto.

Wenn Sie den Authentifizierungstyp ändern, werden die entsprechenden Felder angezeigt. Sie müssen die erforderlichen Informationen eingeben.

Siehe ["Authentifizierungstypen für Protection Center-Benutzerkonten"](#) auf Seite 67.

Siehe ["Benutzerauthentifizierungseinstellungen für Protection Center \(lokal\)"](#) auf Seite 68.

Siehe ["Active Directory- und LDAP-Authentifizierungseinstellungen"](#) auf Seite 69.

- 4 Ändern Sie die Protection Center-Benutzerberechtigungen für das Konto.

Siehe ["Protection Center-Benutzerkontoberechtigungseinstellungen"](#) auf Seite 70.

- 5 Auf der Registerkarte "Zugriff auf unterstützte Produkte" ändern Sie auf die unterstützten Produkte, die das Konto zugreifen kann.

Siehe ["Unterstützte Produktzugriffsberechtigungseinstellungen"](#) auf Seite 75.

- 6 Klicken Sie auf "OK".

Authentifizierungstypen für Protection Center-Benutzerkonten

Sie müssen den Authentifizierungstyp angeben, den Sie für das Protection Center-Benutzerkonto verwenden möchten. Falls Sie beim Bearbeiten eines Protection Center-Benutzerkontos den Authentifizierungstyp ändern, gehen alle Einstellungen der Benutzerauthentifizierung verloren. Sie müssen die entsprechenden Benutzerdetails angeben oder das entsprechende für den neuen Authentifizierungstyp relevante Konto auswählen.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Tabelle 6-5 Authentifizierungstypen für Protection Center-Benutzerkonten

Typ	Beschreibung
Protection Center (lokal)	Bei dem Benutzerkonto handelt es sich um ein lokales Protection Center-Benutzerkonto. Wenn der Benutzer bei Protection Center einloggt, werden der angegebene Benutzername und das Kennwort durch Protection Center authentifiziert. Siehe "Benutzerauthentifizierungseinstellungen für Protection Center (lokal)" auf Seite 68.
Active Directory oder LDAP	Das Protection Center-Benutzerkonto wird einem entsprechenden Benutzerkonto zugewiesen, das bereits in Microsoft Active Directory oder LDAP besteht. Sobald sich der Benutzer bei Protection Center einloggt, werden der Benutzername und das Kennwort zur Authentifizierung an Active Directory oder LDAP weitergeleitet. Siehe "Active Directory- und LDAP-Authentifizierungseinstellungen" auf Seite 69. Bevor Sie ein Active Directory oder LDAP-Benutzerkonto auswählen können, müssen Sie zur Authentifizierung den Active Directory oder LDAP-Server angeben. Siehe "Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung" auf Seite 58.

Benutzerauthentifizierungseinstellungen für Protection Center (lokal)

Wenn ein Protection Center-Benutzerkonto eine lokale Protection Center-Authentifizierung verwendet, müssen Sie den Kontobenzernamen, das Kennwort und die Benutzerdetails angeben. Wenn der Benutzer bei Protection Center einloggt, werden der angegebene Benutzername und das Kennwort durch Protection Center authentifiziert.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Authentifizierungstypen für Protection Center-Benutzerkonten"](#) auf Seite 67.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Tabelle 6-6 Authentifizierungseinstellungen Protection Center (lokal)

Element	Beschreibung
Benutzername	Gibt den Kontobenzutzernamen an. Der Benutzername ist der eindeutige Bezeichner des Protection Center-Benutzerkontos.
Kennwort Kennwort bestätigen	Gibt das Kontokennwort an. In beiden Feldern muss das gleiche Kennwort eingegeben werden. Ein lokales Protection Center-Kennwort muss aus mindestens acht Zeichen bestehen und mindestens drei der folgenden Angaben enthalten: ■ Alphabetische Großbuchstaben (A bis Z) ■ Alphabetische Unicode-Zeichen, die weder Großbuchstaben (A bis Z) noch Kleinbuchstaben (a bis z) sind ■ Numerisches Zeichen (0 bis 9) ■ Nicht alphanumerische Zeichen (~!@#\$\$%^&* _-+=`\\ {}[];:'"<>.,?/)
Vorname	Gibt den Vornamen des Protection Center-Benutzers an.
Nachname	Gibt den Nachnamen des Protection Center-Benutzers an.
E-Mail-Adresse	Gibt die E-Mail-Adresse des Protection Center-Benutzers an. Protection Center versendet automatisch generierte E-Mails, z. B. Berichte oder Benachrichtigungen, an diese Adresse.
Konto deaktivieren	Deaktiviert das Protection Center-Benutzerkonto. Mit dieser Option können Sie vorab Benutzerkonten erstellen, aber die Benutzer können erst nach Ihrer Freigabe auf Protection Center zugreifen. Wenn Sie neue Konten für die Benutzer bereitstellen möchten, müssen Sie nur die entsprechenden Konten aktivieren. Diese Einstellung ist nur dann verfügbar, wenn Sie ein Protection Center-Benutzerkonto ändern.

Active Directory- und LDAP-Authentifizierungseinstellungen

Wenn ein Protection Center-Benutzerkonto die Active Directory- oder LDAP-Authentifizierung verwendet, müssen Sie das entsprechende Active Directory- oder LDAP-Benutzerkonto angeben. Protection Center importiert den entsprechenden Benutzernamen, das Kennwort und andere Benutzerdetails für das neue Protection Center-Benutzerkonto. Diese Details werden aber immer noch auf dem Active Directory- oder LDAP-Server verwaltet und können in Protection Center nicht geändert werden. Wenn der Benutzer bei Protection Center einloggt,

werden seine Angaben, d. h. der Benutzername und das Kennwort, zur Authentifizierung an Active Directory oder LDAP weitergeleitet.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Authentifizierungstypen für Protection Center-Benutzerkonten"](#) auf Seite 67.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Tabelle 6-7 Active Directory- und LDAP-Authentifizierungseinstellungen

Element	Beschreibung
Active Directory- oder LDAP-Kontoname	Gibt den Benutzernamen des Microsoft Active Directory- oder LDAP-Kontos an, das Sie in Protection Center verwenden möchten. Diese Einstellung ist nur dann verfügbar, wenn Sie ein Protection Center-Benutzerkonto erstellen. Dieses Feld ist ein aktives Suchfeld: Es entspricht der Textzeichenfolge, die Sie mithilfe der verfügbaren Konten durch Vornamen, Nachnamen und Benutzernamen eingeben. Protection Center importiert die Kontodetails vom Active Directory- oder LDAP-Server. Leere Felder werden automatisch ausgefüllt.
Benutzername	Gibt den Benutzernamen des angegebenen Active Directory- oder LDAP-Kontos an.
Vorname	Gibt den Vornamen des angegebenen Active Directory- oder LDAP-Kontos an.
Nachname	Gibt den Nachnamen des angegebenen Active Directory- oder LDAP-Kontos an.
E-Mail	Gibt die E-Mail-Adresse des angegebenen Active Directory- oder LDAP-Kontos an. Protection Center versendet automatisch generierte E-Mails, z. B. Berichte oder Benachrichtigungen, an diese Adresse.

Protection Center-Benutzerkontoberechtigungseinstellungen

Protection Center-Berechtigungen steuern den Benutzerzugriff auf die Funktionen von Protection Center. Sie müssen dem Benutzerkonto die Berechtigungen zuweisen, die der Benutzer benötigt, um auf die entsprechenden Protection Center-Funktionen zuzugreifen.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Für jede Funktion von Protection Center können Sie Benutzern Berechtigungen zum Anzeigen oder Verwalten geben. Die Berechtigung zum Anzeigen ermöglicht dem Benutzer einen schreibgeschützten Zugriff auf die Funktion. Der Benutzer kann zwar die Menüoption sehen und auf die entsprechende Seite der Benutzeroberfläche zugreifen, um die aktuellen Einstellungen anzuzeigen, aber keine Änderungen vornehmen. Die Berechtigung zum Verwalten gibt dem Benutzer vollen Zugriff auf die Funktion und die Möglichkeit, die aktuellen Einstellungen zu ändern.

Sie können Benutzerberechtigungen manuell zuweisen, indem Sie einzelne Berechtigungen auswählen, oder Sie können den vollständigen Satz an Berechtigungen aus einem anderen Protection Center-Benutzerkonto kopieren.

Diese Benutzerberechtigungen gelten nur für Funktionen von Protection Center. Sie geben Produktzugriffsrechte an, wenn Sie Links zu unterstützten Produkten einrichten.

Siehe ["Unterstützte Produktzugriffsberechtigungseinstellungen"](#) auf Seite 75.

Tabelle 6-8 Protection Center-Benutzerkontoberechtigungseinstellungen

Element	Beschreibung
Protection Center-Berechtigungen	Enthält die Berechtigungen, die für das Benutzerkonto gelten. Siehe "Protection Center-Benutzerkontoberechtigungen" auf Seite 71.
Berechtigungen kopieren aus	Kopiert die Benutzerberechtigungen aus einem anderen Protection Center-Benutzerkonto. Die entsprechenden Berechtigungen werden als Standardeinstellungen für das Benutzerkonto übernommen. Die Dropdown-Liste enthält alle verfügbaren Protection Center-Benutzerkonten. Wenn Sie das gewünschte Konto auswählen, werden die entsprechenden Berechtigungen aktiviert. Sie können sie an die Anforderungen des neuen Benutzers anpassen. Sie können diese Funktion nicht verwenden, um die Berechtigungen von zwei oder mehr Benutzerkonten auszuwählen und zusammenzuführen. Jedes Mal, wenn Sie diesen Prozess wiederholen und ein Benutzerkonto auswählen, überschreiben die ausgewählten Kontoeinstellungen die vorhandenen Einstellungen.

Protection Center-Benutzerkontoberechtigungen

Protection Center verwendet berechtigungsbasierte Sicherheit, um den Benutzerzugriff auf die Funktionen von Protection Center zu steuern. Sie können jedem Benutzerkonto die Berechtigungen zuweisen, die der Benutzer benötigt, um auf die entsprechenden Protection Center-Funktionen zuzugreifen.

Beispielsweise benötigt der Hauptadministrator für Protection Center vollen Zugriff auf alle Protection Center-Funktionen und hat deshalb alle verfügbaren Berechtigungen. Die meisten Protection Center-Benutzer arbeiten jedoch hauptsächlich mit unterstützten Produkten. Diese Benutzer benötigen keinen Zugriff auf erweiterte Protection Center-Funktionen wie zum Beispiel das Erstellen neuer Protection Center-Benutzerkonten oder das Konfigurieren der Protection Center-Appliance. Solchen Benutzern würde ein reduzierter Satz von Berechtigungen zugewiesen, der ihnen nur Zugriff auf die Funktionen gewährt, die sie für ihre Arbeit benötigen. Sie können die Zugriffsebene für das Verwalten der Protection Center-Funktionen für jeden Benutzer angeben.

Die folgenden Berechtigungen sollten nur vertrauenswürdigen Administratoren gewährt werden:

■ **Benutzerverwaltung**

Diese Berechtigung ermöglicht es dem Administrator, Single-Sign-On-Benutzerzuordnungen zu konfigurieren. Ein Benutzer mit dieser Berechtigung ist in der Lage, auf allen aktivierten Produkte zuzugreifen und Zugriff zu gewähren, einschließlich Zugriff auf Administratorebene.

■ **Unterstützte Produkte**

Diese Berechtigung ermöglicht es einem Benutzer, unterstützte Produkte zu aktivieren und zu deaktivieren. Änderungen an den Produktverbindungen haben Auswirkungen auf die Arbeit anderer Protection Center-Benutzer.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Protection Center-Benutzerkontoberechtigungseinstellungen"](#) auf Seite 70.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Tabelle 6-9 Protection Center-Benutzerkontoberechtigungen

Berechtigung	Beschreibung
Unterstützte Produkte	Ermöglicht das Hinzufügen von unterstützten Produkten zu Protection Center. Sie können unterstützte Produkte nach Bedarf aktivieren und deaktivieren. Siehe "Integrieren unterstützter Produkte" auf Seite 30.
Benutzerverwaltung	Hiermit können Sie Protection Center-Benutzerkonten konfigurieren, um jedem Benutzer Zugriff auf die entsprechenden Protection Center-Funktionen zu geben. Siehe "Über Protection Center-Benutzerkonten" auf Seite 56. Siehe "Einrichten von Protection Center-Benutzerkonten" auf Seite 57.

Berechtigung	Beschreibung
Software-Update	Ermöglicht das Anzeigen der Software-Updates, die heruntergeladen wurden und zur Installation in Protection Center verfügbar sind. Sie können die Updates auswählen, die Sie installieren möchten. Siehe "Infos zu Softwareupdates für Protection Center" auf Seite 77.
Einstellungen	Ermöglicht das Aktivieren bzw. Deaktivieren Sie aller Optionen unter "Einstellungen". Wenn diese Option aktiviert wird, werden die Berechtigungen zum Anzeigen und Verwalten aller Optionen unter "Einstellungen" ausgewählt. Wenn diese Option deaktiviert wird, werden alle Berechtigungen für alle Optionen unter "Einstellungen" entfernt.
Active Directory und LDAP	Ermöglicht das Angeben des Microsoft Active Directory- oder LDAP-Servers, den Protection Center verwendet, um Benutzerkonten zu authentifizieren. Siehe "Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung" auf Seite 58.
Backup	Ermöglicht das Konfigurieren der Protection Center-Backups. Protection Center verwendet Symantec Backup Exec System Recovery zum Erstellen regelmäßiger Backups. Siehe "Info zu Protection Center-Backup und -Wiederherstellung" auf Seite 83.
Community-Statistik	Ermöglicht die Angabe, ob Protection Center Daten zur Community-Statistik sammelt und für Diagnosenzwecke an Symantec sendet. Siehe "Community-Statistik-Einstellungen" auf Seite 96.
Datum/Zeit	Ermöglicht das Einstellen von Datum und Uhrzeit der Protection Center-Appliance. Siehe "Datums- und Uhrzeiteinstellungen" auf Seite 97.
E-Mail	Ermöglicht das Konfigurieren der E-Mail-Einstellungen für Protection Center. Protection Center verwendet E-Mails, um Warnmeldungen an den Administrator zu senden, wenn Elemente möglicherweise dessen Eingreifen erfordern. Siehe "E-Mail-Einstellungen" auf Seite 97.
LiveUpdate	Geben Sie hier an, ob für Protection Center-Software-Updates der LiveUpdate-Server von Symantec oder ein lokaler LiveUpdate-Server verwendet werden soll. Wenn Sie einen lokalen LiveUpdate-Server verwenden, können Sie die entsprechenden Serverdetails angeben. Siehe "Angabe des LiveUpdate-Servers" auf Seite 80.
Nachrichtenprotokollierung	Ermöglicht die Wahl der von Protection Center verwendeten Protokollierungsstufe: normale oder ausführliche Protokollierung. Siehe "Nachrichtenprotokollierungseinstellungen" auf Seite 99.

Berechtigung	Beschreibung
Netzwerk	Ermöglicht das Konfigurieren der Netzwerkeinstellungen für Protection Center. Siehe "Netzwerkkonfigurationseinstellungen" auf Seite 100.
Kennwortänderung	Hiermit können Sie Ihr Kennwort jederzeit ändern. Diese Funktion gilt nur für lokal authentifizierte Konten. Konten, die Active Directory- oder LDAP-Authentifizierung verwenden, können nicht innerhalb von Protection Center geändert werden. Siehe "Ändern des Kennworts für Ihr Benutzerkonto" auf Seite 21.
Produkterkennung	Ermöglicht das Erkennen der von Protection Center unterstützten Produkte, die im Netzwerk installiert sind. Siehe "Erkennen unterstützter Produkte im Netzwerk" auf Seite 34.
Proxy	Ermöglicht das Konfigurieren eines HTTP-Proxy-Servers für Protection Center. Ein Proxy-Server trägt dazu bei, die Sicherheit von Protection Center zu erhöhen. Siehe "Proxy-Server-Einstellungen" auf Seite 100.
Bereinigen	Hiermit können Sie das Bereinigen von älteren Daten in der Protection Center-Datenbank steuern. Sie können die Anzahl der Tage festlegen, für die Daten in der Datenbank gespeichert werden. Siehe "Datenbereinigungseinstellungen" auf Seite 102.
Herunterfahren	Herunterfahren oder Neustarten von Protection Center. Siehe "Herunterfahren oder Neustarten von Protection Center" auf Seite 27.
Support-Diagnosen	Hiermit können Sie Diagnoseninformationen sammeln und für Support-Zwecke an Symantec senden. Siehe "Hilfe vom Symantec-Support" auf Seite 115.
Workflow	Ermöglicht das Konfigurieren von mit Protection Center zu verwendenden Workflows. Siehe "Konfigurieren der Verwaltungseinstellungen für einen Workflow" auf Seite 154. Siehe "Verfügbare Workflows in Protection Center" auf Seite 159.
Systemprotokolle	Ermöglicht das Anzeigen des Berichts "Systemprotokolle". Siehe "Anzeigen eines Berichts" auf Seite 136.

Unterstützte Produktzugriffsberechtigungseinstellungen

Sie müssen die aktivierten Produkte angeben, auf die das Protection Center-Benutzerkonto über Protection Center zugreifen kann. Wenn ein Konto Zugriff auf ein Produkt hat, kann der Benutzer Daten aus diesem Produkt in Protection Center-Berichten anzeigen. Wenn ein Konto keinen Zugriff auf ein aktiviertes Produkt hat, werden die Daten aus diesem Produkt nicht in Protection Center-Berichte einbezogen, die der Benutzer anzeigt.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Erstellen von Protection Center-Benutzerkonten"](#) auf Seite 64.

Siehe ["Ändern eines Protection Center-Benutzerkontos"](#) auf Seite 66.

Für jedes aktivierte Produkt, auf das das Konto zugreifen kann, müssen Sie ein Produktbenutzerkonto angeben, den das Protection Center-Benutzerkonto zugeordnet werden soll. Das Produktbenutzerkonto definiert den einzelnen Single-Sign-On-Zielbenutzer im integrierten Produkt. Wenn der Protection Center-Benutzer Single-Sign-On verwendet, um auf das integrierte Produkt zuzugreifen, werden sie beim Produkt unter Verwendung des angegebenen Kontos eingeloggt.

Tabelle 6-10 Unterstützte Produktzugriffsberechtigungseinstellungen

Element	Beschreibung
Integriertes Produkt	Gibt die Produktinstanz an, für die Sie dem Protection Center-Benutzerkonto Zugriff gewähren möchten.
Verknüpfter Benutzername	Gibt das Produktbenutzerkonto an, das Sie mit dem Protection Center-Benutzerkonto verknüpfen möchten.
Entfernen	Ermöglicht das Hinzufügen oder Entfernen eines verknüpften Produkts. Die entsprechende Option wird angezeigt: ■ Hinzufügen Fügt den angegebenen Produkthost und das verknüpfte Benutzerkonto dem Protection Center-Benutzerkonto hinzu. ■ Entfernen Entfernt den Produkthost und das verknüpfte Benutzerkonto aus dem Protection Center-Benutzerkonto.

Löschen eines Protection Center-Benutzerkontos

Sie können ein Protection Center-Benutzerkonto löschen, falls das Konto nicht mehr benötigt wird. Das einzige Konto, das nicht gelöscht werden kann, ist das SPC_Admin-Konto. Das Löschen eines Protection Center-Kontos hat keine Auswirkungen auf ein entsprechendes Active Directory- oder LDAP-Konto. Es hat keine Auswirkungen auf die zugeordneten Benutzerkonten integrierter Produkte.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Einrichten von Protection Center-Benutzerkonten"](#) auf Seite 57.

So löschen Sie ein Protection Center-Benutzerkonto

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Benutzerverwaltung".
- 2 Wählen Sie auf der Benutzerverwaltungsseite das Konto aus, das Sie löschen möchten, und klicken Sie anschließend auf "Löschen".
- 3 Klicken Sie im Dialogfeld "Benutzerkonto löschen" "Benutzer löschen".
Das Benutzerkonto wird von der Benutzerverwaltungsseite entfernt.

Verwalten von Protection Center-Softwareupdates

In diesem Kapitel werden folgende Themen behandelt:

- [Infos zu Softwareupdates für Protection Center](#)
- [Verwalten von Protection Center-Softwareupdates](#)
- [Angabe des LiveUpdate-Servers](#)
- [LiveUpdate-Einstellungen](#)

Infos zu Softwareupdates für Protection Center

Protection Center nutzt LiveUpdate, um die Softwarekomponenten auf dem neuesten Stand zu halten. Außerdem verwendet Protection Center LiveUpdate, um die Informationen zu aktualisieren, die Protection Center für das Zusammenwirken mit unterstützten Produkten benötigt.

Wenn Protection Center nicht auf das Internet zugreifen soll (direkt oder über einen Proxy-Server), können Sie Updates manuell herunterladen und installieren.

Siehe "[Manuelles Aktualisieren der Protection Center-Software](#)" auf Seite 107.

Es können folgende Updates verfügbar sein:

- Updates für wichtige Microsoft-Produktkomponenten von Protection Center, wie zum Beispiel Microsoft Windows Server, Internet Information Services (IIS) und SQL Server.

Protection Center muss so konfiguriert sein, dass der lokale Windows-Update-Server zum Herunterladen von Windows-Updates verwendet wird. Sie können den lokalen Windows-Update-Server über die Systemsteuerung konfigurieren.

Siehe ["Zugreifen auf die Protection Center-Systemsteuerung"](#) auf Seite 107.

Siehe ["Windows-Betriebssystem aktivieren"](#) auf Seite 111.

- Updates und Fixes für Software, Berichte, Dokumentation und anderen Komponenten von Protection Center.
- Neue und aktualisierte Konfigurationsdaten für unterstützte Produkte.

Siehe ["Verwalten von Protection Center-Softwareupdates"](#) auf Seite 78.

Symantec empfiehlt, dass Sie Protection Center mindestens einmal täglich aktualisieren, um Defekte und Sicherheitslücken zu verhindern.

Möglicherweise müssen Sie Änderungen an Ihrer Protection Center-Installation vornehmen, um sie an die Bedürfnisse Ihres Unternehmens anzupassen. Weitere Informationen finden Sie im Handbuch zur Größenaufteilung und Skalierbarkeit von Symantec Protection Center.

Hinweis: Updates für unterstützte Produkte werden automatisch in Protection Center installiert, sobald sie heruntergeladen wurden. Sie können die Installation nicht verzögern oder planen.

Verwalten von Protection Center-Softwareupdates

Protection Center lädt neue Updates vom LiveUpdate-Server in regelmäßigen Abständen herunter. Sie können jederzeit den Standardzeitplan überschreiben und nach neuen Updates suchen. Auf der Software-Update-Verwaltungsseite werden Details zu den Software-Updates für Protection Center angezeigt, die zur Installation verfügbar sind. Sie können die Updates auswählen, die Sie auf Protection Center installieren möchten. Sie können die Software-Updates auch anzeigen, die bereits auf Protection Center installiert sind.

Siehe ["Infos zu Softwareupdates für Protection Center"](#) auf Seite 77.

Siehe ["Angabe des LiveUpdate-Servers"](#) auf Seite 80.

Wenn Sie ein Software-Update für die Installation auswählen, wählt Protection Center automatisch alle relevanten erforderlichen Updates aus. Diese erforderlichen Updates werden in der entsprechenden Reihenfolge installiert, bevor das ausgewählte Software-Update installiert wird.

Hinweis: Protection Center führt ein Backup durch, bevor die Installation des Software-Updates beginnt. Dieser Prozess unterbricht möglicherweise die Aktivitäten von Protection Center-Benutzern. Der Administrator, der den Installationsprozess beginnt, sieht ein Dialogfeld, das den aktuellen Status der Installation anzeigt, aber die anderen Benutzer sehen nichts. Wenn Sie andere Protection Center-Benutzer über ein Software-Update informieren möchten, müssen Sie sie manuell benachrichtigen.

So zeigen Sie Einzelheiten der Protection Center-Software-Updates an

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Softwareupdate".
- 2 Auf der Software-Update-Verwaltungsseite klicken Sie auf eine der folgenden Optionen:

Verfügbare Updates	Zeigt die Einzelheiten der Software-Updates an, die vom LiveUpdate-Server heruntergeladen wurden und für die Installation auf Protection Center verfügbar sind.
Installierte Updates	Zeigt die Einzelheiten der Softwareupdates an, die auf Protection Center installiert wurden.

- 3 (Optional) Klicken Sie in der Beschreibungsspalte auf "Mehr", um weitere Informationen zu bestimmten Softwareupdates zu erhalten.

Die Beschreibung erweitert sich, um alle verfügbaren Informationen für das Softwareupdate anzuzeigen.

So suchen Sie sofort nach Updates

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Softwareupdate".
- 2 Auf der Software-Update-Verwaltungsseite auf der Registerkarte Verfügbare Updates, klicken Sie auf "Jetzt nach Updates suchen".

Protection Center durchsucht den LiveUpdate-Server und lädt alle neuen Updates sofort herunter. Das Dialogfeld "Status des manuellen Update" zeigt den aktuellen Status des Prozesses an.

So installieren Sie Protection Center-Software-Updates

- 1 Klicken Sie in Protection Center im Menü "Admin" auf "Softwareupdate".
- 2 Klicken Sie auf der Software-Update-Verwaltungsseite auf der Registerkarte "Verfügbare Updates" auf die Updates, die Sie installieren möchten.

- 3 Klicken Sie auf "Updates installieren".
- 4 Im Dialogfeld "Updates installieren" prüfen Sie, ob die richtigen Softwareupdates aufgelistet werden und klicken Sie dann auf "Updates installieren", um die Installation zu bestätigen.

Das Dialogfeld "Protection Center sichern" zeigt den aktuellen Status des Backup-Prozesses an. Wenn das Backup abgeschlossen ist, werden die Softwareupdates installiert. Das Dialogfeld "Status der Updateinstallation" zeigt den Status der Softwareupdate-Installation an.

Wenn die Installation abgeschlossen ist, schließt sich das Dialogfeld "Status der Updateinstallation". Die installierten Updates werden von der Registerkarte "Verfügbare Updates" entfernt und auf der Registerkarte "Installierte Updates" angezeigt.

Angabe des LiveUpdate-Servers

In Protection Center können Sie den LiveUpdate-Server angeben, der für Protection Center-Software-Updates verwendet werden soll. Sie können den Symantec LiveUpdate-Server oder einen lokalen LiveUpdate-Server verwenden. Der Symantec LiveUpdate-Server wird vorkonfiguriert und Sie müssen keine weitere Konfiguration durchführen. Wenn Sie LiveUpdate-Server innerhalb der Firewall Ihres Unternehmens lokal einrichten, kann Protection Center eine davon verwenden. Wenden Sie sich an Ihren Systemadministrator für weitere Information zu lokalen verfügbaren LiveUpdate-Servern.

Der Port, den LiveUpdate für das Herunterladen von Updates verwendet, hängt vom Transportprotokoll ab. Für HTTP verwenden Sie Port 80. Für HTTPS verwenden Sie Port 443. Für FTP verwenden Sie Port 21. Sie müssen sicherstellen, dass der entsprechende Port verfügbar ist.

Hinweis: Diese Funktion unterstützt die Verwendung eines HTTP-Proxy-Servers zum Zugriff auf Updates. Ein FTP-Proxy-Server wird nicht unterstützt.

Siehe ["Proxy-Server-Einstellungen"](#) auf Seite 100.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Protection Center durchsucht den LiveUpdate-Server jede Nacht um Mitternacht. Sie können diese Zeit und Frequenz nicht ändern. Wenn ein Update gefunden wird, lädt Protection Center automatisch das Update herunter. Protection Center schickt dann eine Benachrichtigung zum Newsfeed, um Sie zu informieren, dass ein Update für die Installation verfügbar ist. Sie können das Update dann installieren.

Siehe ["Infos zu Softwareupdates für Protection Center"](#) auf Seite 77.

Siehe ["Verwalten von Protection Center-Softwareupdates"](#) auf Seite 78.

So geben Sie den LiveUpdate-Server an

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "LiveUpdate".
- 2 Geben Sie auf der LiveUpdate-Einstellungsseite an, wie Protection Center auf LiveUpdate zugreift.
 Siehe ["LiveUpdate-Einstellungen"](#) auf Seite 81.
- 3 Klicken Sie auf "Änderungen speichern".

LiveUpdate-Einstellungen

In Protection Center können Sie den zu verwendenden LiveUpdate-Server angeben. Sie können wählen, ob für Protection Center-Software-Updates der LiveUpdate-Server von Symantec oder ein lokaler LiveUpdate-Server verwendet werden soll. Wenn Sie einen lokalen LiveUpdate-Server verwenden, können Sie die entsprechenden Serverdetails angeben. Wenn Sie nicht möchten, dass Protection Center entweder direkt oder über einen Proxy-Server auf das Internet zugreift, können Sie die Funktion "LiveUpdate" deaktivieren. Sie können die benötigten Software-Updates manuell herunterladen und über die Protection Center-Systemsteuerung installieren.

Siehe ["Infos zu Softwareupdates für Protection Center"](#) auf Seite 77.

Siehe ["Verwalten von Protection Center-Softwareupdates"](#) auf Seite 78.

Siehe ["Angabe des LiveUpdate-Servers"](#) auf Seite 80.

Tabelle 7-1 LiveUpdate-Einstellungen

Element	Beschreibung
Direkt von Symantec	Gibt an, dass Protection Center die entsprechenden Software-Updates direkt vom LiveUpdate-Server von Symantec herunterlädt. Sie brauchen keine weitere Konfiguration durchzuführen.

Element	Beschreibung
Verwenden eines LiveUpdate Admin-Servers	Gibt an, dass Protection Center einen lokal innerhalb Ihrer Firewall ausgeführten LiveUpdate-Server verwendet. Protection Center lädt die entsprechenden Software-Updates vom angegebenen Server herunter, statt den LiveUpdate-Server von Symantec zu nutzen. Sie müssen den zu verwendenden lokalen LiveUpdate-Server wie folgt angeben: ■ "Host" - der Servername, einschließlich des vollständig qualifizierten Domännennamens. Alternativ können Sie die IP-Adresse des LiveUpdate-Server-Hosts verwenden. ■ "Pfad" - der Netzwerkpfad zum Host-Server. ■ "Protokoll" - das Transportprotokoll, das Protection Center zum Herunterladen von Software-Updates vom Host-Server verwendet. Die verfügbaren Optionen sind: "HTTP", "HTTPS" und "FTP". ■ "Port" - der auf dem Host-Server zu verwendende Port. Die Port-Nummer hängt vom verwendeten Transportprotokoll ab. Geben Sie für HTTP Port 80 ein, für HTTPS Port 443 und für FTP Port 21. ■ "Benutzername" - der Benutzername eines Administratorkontos auf dem Host-Server. ■ "Kennwort" - das Kennwort für das Administratorkonto auf dem Host. Mithilfe der Schaltfläche "LiveUpdate-Einstellungen testen" können Sie die angegebenen Einstellungen überprüfen.
LiveUpdate nicht verwenden	Gibt an, dass Protection Center auf keinen LiveUpdate-Server zugreift. Sie müssen die benötigten Software-Updates manuell herunterladen. Sie können Software-Updates über die Protection Center-Systemsteuerung manuell installieren. Siehe "Manuelles Aktualisieren der Protection Center-Software" auf Seite 107.

Sichern und Wiederherstellen von Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Protection Center-Backup und -Wiederherstellung](#)
- [Planen von automatischen Backups](#)
- [Backup-Einstellungen](#)
- [Wiederherstellen von Protection Center](#)
- [Erstellen des Symantec Recovery Disk](#)
- [Testen des Symantec Recovery Disk](#)

Info zu Protection Center-Backup und -Wiederherstellung

Protection Center umfasst Symantec Backup Exec System Recovery für Backup und Wiederherstellung von Daten und System. Sie können einen Backup-Zeitplan so konfigurieren, dass automatisch vollständige Backups und inkrementelle Backups der Protection Center-Festplatte erstellt werden. Ein vollständiges Backup ist ein Image der gesamten Protection Center-Appliance. Das Image umfasst das Betriebssystem und die dazugehörigen Programme und alle Daten in der Protection Center-Datenbank. Ein inkrementelles Backup enthält nur die Daten und die Dateien, die neu sind oder seit dem letzten Backup geändert wurden. Ein

inkrementelles Backup nimmt viel weniger Speicherplatz ein als ein vollständiges Backup, weil nicht jedes Mal die gesamte Festplatte kopiert wird.

Siehe "[Planen von automatischen Backups](#)" auf Seite 85.

Siehe "[Backup-Einstellungen](#)" auf Seite 85.

Das erste Backup, das jede Woche geplant wird, ist ein vollständiges Backup; alle weiteren Backups, die während der gleichen Woche geplant werden, sind inkrementelle Backups. Protection Center behält Backup-Dateien für die laufende Woche und für die vorherigen zwei Wochen bei. Alle älteren Backup-Dateien werden entsprechend dem Bereinigungszeitplan bereinigt, den Sie in Protection Center konfiguriert haben.

Möglicherweise müssen Sie Änderungen an Ihrer Protection Center-Installation vornehmen, um sie an die Bedürfnisse Ihres Unternehmens anzupassen. Weitere Informationen finden Sie im Handbuch zur Größenaufteilung und Skalierbarkeit von Symantec Protection Center.

Wenn ein Problem innerhalb von Protection Center auftritt, wie zum Beispiel eine beschädigte Datei, können Sie das Backup-Image zur vorhandenen Protection Center-Appliance wiederherstellen. Wenn die Protection Center-Festplatte ausfällt, können Sie diese Festplatte austauschen und das Backup-Image auf dem neuen Laufwerk wiederherstellen. Wenn Sie Protection Center aus Ihren Backups wiederherstellen, wird zuerst das vollständige Backup-Image installiert. Anschließend werden die inkrementellen Backups nacheinander in der Reihenfolge verarbeitet, in der sie erstellt wurden. Wenn das neueste Backup ein vollständiges Image ist, müssen keine inkrementellen Backups wiederhergestellt werden.

Siehe "[Wiederherstellen von Protection Center](#)" auf Seite 87.

Um Protection Center wiederherzustellen, benötigen Sie einen Symantec Recovery Disk. Dieser Datenträger ist eine CD/DVD, die Sie verwenden, um die Appliance zu starten und die Protection Center-Festplatte aus den gespeicherten Backups wiederherzustellen. Sie müssen den Datenträger erstellen, indem Sie Software von der Protection Center-Seite auf der Symantec-Website auf Ihre eigene CD/DVD brennen. Die Protection Center-Seite befindet sich unter folgender URL:

<http://go.symantec.com/protection-center>

Um sicherzustellen, dass der Wiederherstellungsdatenträger verfügbar ist, wenn Sie ihn benötigen, sollten Sie den Wiederherstellungsdatenträger beim Konfigurieren der Backups erstellen.

Siehe "[Erstellen des Symantec Recovery Disk](#)" auf Seite 90.

Siehe "[Testen des Symantec Recovery Disk](#)" auf Seite 91.

Planen von automatischen Backups

Sie können einen Backup-Zeitplan so konfigurieren, dass automatisch vollständige Backups (wöchentlich) und inkrementelle Backups (täglich) der Protection Center-Festplatte erstellt werden. Der Wochenzeitplan beginnt am Sonntag. Das erste Backup, das im Wochenzeitplan erscheint, ist das wöchentliche vollständige Backup. Alle weiteren Backups, die im Wochenzeitplan angegeben werden, sind inkrementelle Backups. Die einzige Ausnahme tritt auf, wenn Sie den Backup-Zeitplan zum ersten Mal konfigurieren: Das erste Backup ist immer ein vollständiges Backup, unabhängig davon, an welchem Tag es erstellt wird.

Beachten Sie, dass Protection Center Backups im Hintergrund erstellt: Dabei werden keine Benachrichtigungen gesendet, um Sie über den Status von Backup-Ereignissen zu informieren. Im Newsfeed wird jedoch eine Benachrichtigung angezeigt, wenn ein Backup fehlschlägt.

Um vollständige und inkrementelle Backups zu verwalten, müssen Sie das Volumen der eingehenden Daten kennen und die Rate, mit der sich die Daten ändern. Wenn Protection Center normalerweise jeden Tag eine große Menge Daten speichert, sollten Sie ein tägliches inkrementelles Backup konfigurieren. Wenn Protection Center nicht jeden Tag große Mengen Daten speichert oder ändert, können Sie das inkrementelle Backup ein- oder zweimal pro Woche ausführen.

Jedes inkrementelle Backup ist auf das vorhergehende inkrementelle Backup angewiesen, um zu funktionieren. Das bedeutet: Wenn ein inkrementelles Backup fehlschlägt, kann keines der danach erstellten inkrementellen Backups wiederhergestellt werden. Deshalb sollten Sie sofort eingreifen, wenn Sie eine Benachrichtigung über ein fehlgeschlagenes Backup erhalten.

Siehe ["Info zu Protection Center-Backup und -Wiederherstellung"](#) auf Seite 83.

So planen Sie automatische Backups

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Backup".
- 2 Geben Sie auf der Seite "Backup-Einstellungen" die entsprechenden Einstellungen an.
Siehe ["Backup-Einstellungen"](#) auf Seite 85.
- 3 Klicken Sie auf "Änderungen speichern".

Backup-Einstellungen

Sie können Einstellungen für Backup-Dateispeicherort, kennwortgeschützte Backups und Zeitpläne für inkrementelle Backups konfigurieren.

Siehe ["Planen von automatischen Backups"](#) auf Seite 85.

Tabelle 8-1 Backup-Einstellungen

Element	Beschreibung
Einstellungen für den Speicherort der Backup-Datei	Gibt den Backup-Dateispeicherort und die dazugehörigen Identifikationsdaten für den Zugriff an. Sie müssen Folgendes angeben: ■ Speicherort Der Ort, an dem Ihre Protection Center-Backup-Dateien gespeichert werden soll. Geben Sie den vollständigen Pfad zum vorgesehenen Speicherort für die Backup-Dateien an. Sie müssen Backup-Dateien in einem gemeinsam genutzten Netzwerkordner speichern. Geben Sie den Pfadnamen im Format <code>\\server\share</code> an. ■ Identifikationsdaten bereitstellen Wenn diese Option aktiviert ist, gibt sie an, dass der Netzwerkfreigabeort eine Authentifizierung erfordert. ■ Benutzername Der Benutzername des Kontos, das Sie für das Einloggen beim Backup-Netzwerkfreigabeort verwenden möchten. Geben Sie den Benutzernamen zusammen mit dem Domänennamen oder dem Arbeitsgruppennamen an. Trennen Sie die zwei Namen mit einem umgekehrten Schrägstrich. ■ Kennwort Das Kennwort des Kontos, das Sie für das Einloggen beim Netzwerkfreigabeort verwenden möchten.
Backup-Datenwörterbuch	Gibt das Kennwort an, das angegeben werden muss, um Protection Center aus den Backup-Dateien wiederherzustellen. Um die Sicherheit zu gewährleisten, müssen alle Backup-Dateien kennwortgeschützt sein. Sie müssen Folgendes angeben: ■ Kennwort ■ Kennwort bestätigen

Element	Beschreibung
Einstellungen für den Backup-Zeitplan	Gibt den Backup-Zeitplan an. Damit die Protection Center-Appliance nicht zu stark belastet wird, empfiehlt Symantec, dass Sie den Backup-Prozess außerhalb der normalen Arbeitszeiten ausführen. Sie können Folgendes angeben: ■ Uhrzeit Die Uhrzeit, zu der der Backup-Prozess an den angegebenen Tagen gestartet wird. Die Zeit entspricht der Serverzeit und wird unter Verwendung einer 24-Stunden-Uhr angegeben. ■ Wochentage Die Wochentage, an denen inkrementelle Backups erstellt werden. Sie können die Wochentage angeben, an denen der Backup-Prozess ausgeführt werden soll. Beispielsweise haben sie die Möglichkeit, alle Wochentage auszuwählen, aber das Wochenende zu überspringen, an dem die Datenänderungen minimal sind. Das erste Backup, das nach dem Zeitplan gemacht wird, ist ein vollständiges Backup-Image. Ein vollständiges Backup wird jede Woche am selben Tag und zur selben Zeit erstellt. Alle weiteren Backups im Zeitplan sind inkrementelle Backups.

Wiederherstellen von Protection Center

Um Protection Center aus einer Backup-Datei wiederherzustellen, müssen Sie den Symantec Recovery Disk verwenden. Der Symantec Recovery Disk verwendet ein eigenes Betriebssystem und umfasst sämtliche Software, die Sie benötigen, um Protection Center wiederherzustellen. Der Symantec Recovery Disk benötigt nur Zugriff auf die Festplatte oder Netzwerkadresse, die Ihre Backup-Dateien enthält. Wenn Sie beschließen, ein Backup wiederherzustellen, installiert der Symantec Recovery Disk das entsprechende Image auf der Protection Center-Festplatte. Die wiederhergestellten Daten umfassen das Protection Center-Appliance-Betriebssystem, die dazugehörigen Programme und alle Daten in der Protection Center-Datenbank.

Siehe "[Info zu Protection Center-Backup und -Wiederherstellung](#)" auf Seite 83.

Der Symantec Recovery Disk wird nicht mit Protection Center geliefert: Sie müssen den Symantec Recovery Disk selbst erstellen. Sie können das ISO-Image von der Protection Center-Seite auf der Symantec-Website herunterladen und auf eine leere CD/DVD brennen. Die Protection Center-Seite befindet sich unter folgender URL:

<http://go.symantec.com/protection-center>

Um sicherzustellen, dass der Wiederherstellungsdatenträger verfügbar ist, wenn Sie ihn benötigen, sollten Sie den Wiederherstellungsdatenträger beim Konfigurieren der Backups erstellen.

Siehe ["Erstellen des Symantec Recovery Disk"](#) auf Seite 90.

Wenn Sie Protection Center wiederherstellen möchten, stellen Sie sicher, dass Sie Administratorzugriff auf die entsprechenden Backup-Dateien haben, weil alle Backup-Dateien kennwortgeschützt sind. Die Backup-Dateien müssen auf einem freigegebenen Netzlaufwerk gespeichert werden.

Wenn Sie Protection Center wiederherstellen, wird normalerweise das volle System wiederhergestellt. Diese Option verwendet die Systemindexdatei und stellt das neueste Backup wieder her. Wenn Sie jedoch das neueste Backup nicht für geeignet halten, können Sie beschließen, die Daten aus einer früheren Backup-Datei wiederherzustellen.

Beachten Sie Folgendes, wenn Sie die zu verwendende Backup-Datei wählen:

- V2i-Dateien sind vollständige Backups.
- iv2i-Dateien sind inkrementelle Backups.
- Sie können das entsprechende Backup anhand der Zeitstempel für die vollständigen Backup-Dateien und die inkrementellen Backups identifizieren.
- Wenn Sie die Daten aus einem inkrementellen Backup (einer iv2i-Datei) wiederherstellen, werden alle erforderlichen früheren Backup-Dateien ebenfalls wiederhergestellt.

So stellen Sie Protection Center wieder her

- 1 Stellen Sie sicher, dass in der Startgerätefolge der Protection Center-Appliance die CD/DVD zuerst gestartet wird.
- 2 Vergewissern Sie sich, dass keine externen USB- oder eSATA-Geräte mit der Anwendung verbunden sind.
- 3 Starten Sie die Protection Center-Appliance vom Symantec Recovery Disk, indem Sie den Datenträger in Ihren Computer einlegen, bevor Sie ihn einschalten.
- 4 Wählen Sie im Dialogfeld "Sprache auswählen" die Sprache aus, die Sie verwenden möchten, und klicken Sie dann auf "OK".
- 5 Lesen Sie die Lizenzvereinbarung und klicken Sie dann auf "Akzeptieren".
- 6 Wenn Sie zum Starten von Netzwerkdiensten aufgefordert werden, klicken Sie auf "Ja".
- 7 Klicken Sie auf der Registerkarte "Wiederherstellen" auf "Recover My Computer".

- 8** Lesen Sie die Informationen auf der Begrüßungsseite "Recover My Computer Wizard" und klicken Sie auf "Weiter".
- 9** Klicken Sie im Dialogfeld "Select a Recovery Point to Restore" auf "Map a Network Drive".
- 10** Geben Sie im Dialogfeld "Netzlaufwerk zuordnen" das Laufwerk und den Ordner an, die Sie verwenden möchten, und klicken Sie dann auf "OK".
- 11** Sie haben folgende Möglichkeiten:

So stellen Sie das letzte Backup wieder her	Wählen Sie in der Dropdown-Liste "View recovery points by" die Option "System". Navigieren Sie zum Backup-Ordner und wählen Sie die .sv2i-Datei aus.
So stellen Sie ein früheres Backup wieder her	Wählen Sie in der Dropdown-Liste "View recovery points by" die Option "Filename". Navigieren Sie zum Backup-Ordner und wählen Sie den Wiederherstellungspunkt aus, den Sie verwenden möchten.
- 12** Wenn Sie zur Eingabe des Kennworts für die Backup-Datei aufgefordert werden, geben Sie das Kennwort ein und klicken Sie auf "OK".
- 13** Klicken Sie auf "Weiter".
- 14** (Optional) Wählen Sie im Dialogfeld "Initialize Disk Partition Structures" den entsprechenden Datenträger aus und klicken Sie dann auf "OK".

Dieser Schritt tritt immer bei neuen Systemen und gelegentlich bei zurückgesetzten Systemen auf.
- 15** Deaktivieren Sie im Dialogfeld "Drives to Recover" die Option "Verify recovery point before restore".
- 16** Wählen Sie das Laufwerk, das Sie wiederherstellen möchten.
- 17** Klicken Sie auf "Bearbeiten" und aktivieren Sie dann im Dialogfeld "Edit Target Drive and Options" die Option "Restore Master Boot Record".
- 18** Klicken Sie auf "OK" und anschließend auf "Weiter".
- 19** Deaktivieren Sie im Dialogfeld "Completing the recover My Computer Wizard" die Option "Reboot when finished".

- 20 Vergewissern Sie sich, dass alle Einstellungen korrekt sind, und klicken Sie auf Fertig stellen, um die Wiederherstellung zu starten.

Die Fortschrittsleiste für die Wiederherstellung zeigt an, zu wie viel Prozent der Wiederherstellungsvorgang abgeschlossen ist und wie viel Zeit noch verbleibt.

- 21 Wenn der Wiederherstellungsvorgang abgeschlossen ist, klicken Sie im Dialogfeld auf "Schließen".

In der letzten Meldung des abschließenden Dialogfelds werden Sie darauf hingewiesen, dass nach dem Schließen der Anwendung die Appliance neu gestartet werden muss.

- 22 Klicken Sie auf "Ja".

Erstellen des Symantec Recovery Disk

Sie müssen den Symantec Recovery Disk zum Starten der Protection Center-Appliance verwenden, wenn Sie ein Backup von Protection Center wiederherstellen möchten.

Siehe "[Wiederherstellen von Protection Center](#)" auf Seite 87.

So erstellen Sie den Symantec Recovery Disk

- 1 Laden Sie die ISO-Datei für den Symantec Recovery Disk von einem Computer aus herunter, der über einen Internetzugang, einen CD/DVD-Brenner und CD/DVD-Brennsoftware verfügt.

Auf die ISO-Datei können Sie über die Protection Center-Seite auf der Symantec-Website unter folgender URL zugreifen:

<http://go.symantec.com/protection-center>

- 2 Verwenden Sie CD/DVD-Brennsoftware, um die ISO-Datei für den Symantec Recovery Disk auf eine leere CD/DVD zu brennen.
- 3 Testen Sie die Symantec Recovery Disk-CD/DVD.

Siehe "[Testen des Symantec Recovery Disk](#)" auf Seite 91.

- 4 Nachdem Sie die Appliance gestartet haben, überprüfen Sie, ob die Netzwerktreiber richtig funktionieren und Sie auf den Speicherort der Backup-Dateien zugreifen können.

Testen des Symantec Recovery Disk

Nachdem Sie Ihre Symantec Recovery Disk-CD/DVD erstellt haben, sollten Sie sie testen, um sicherzustellen, dass die Wiederherstellungsumgebung auf Ihrem Host richtig ausgeführt wird.

Siehe ["Wiederherstellen von Protection Center"](#) auf Seite 87.

Siehe ["Erstellen des Symantec Recovery Disk"](#) auf Seite 90.

Durch Testen des Symantec Recovery Disk können Sie die folgenden Arten von Problemen identifizieren und lösen:

- Sie können den Symantec Recovery Disk nicht starten.
- Sie haben nicht die notwendigen Speichertreiber, um auf die benötigten Backup-Dateien zuzugreifen.
- Sie benötigen Informationen über Ihr System, um den Symantec Recovery Disk ausführen zu können.

Sie können auf die Hilfe für den Symantec Recovery Disk zugreifen, indem Sie in der unteren linken Ecke der Startseite auf den Link "Hilfe" klicken.

So testen Sie den Symantec Recovery Disk

- 1 Starten Sie den Protection Center-Computer unter Verwendung des Symantec Recovery Disk.
- 2 Führen Sie eine Scheinwiederherstellung einer Backup-Datei aus, die auf einem freigegebenen Netzlaufwerk gespeichert ist, um die Verbindung zu testen.

Protection Center unterstützt nicht das Speichern von Backup-Dateien auf lokalen Laufwerken oder auf CD/DVD.

- 3 Entfernen Sie den Symantec Recovery Disk.

Konfigurieren der Protection Center-Einstellungen

In diesem Kapitel werden folgende Themen behandelt:

- [Protection Center-Konfigurationseinstellungen](#)
- [Zugreifen auf die Protection Center-Konfigurationseinstellungen](#)
- [Community-Statistik-Einstellungen](#)
- [Datums- und Uhrzeiteinstellungen](#)
- [E-Mail-Einstellungen](#)
- [Nachrichtenprotokollierungseinstellungen](#)
- [Netzwerkkonfigurationseinstellungen](#)
- [Proxy-Server-Einstellungen](#)
- [Datenbereinigungseinstellungen](#)

Protection Center-Konfigurationseinstellungen

Mit den Protection Center-Konfigurationseinstellungen können Sie Protection Center entsprechend der Umgebung und der Bedürfnisse des Unternehmens konfigurieren.

Alle Protection Center-Konfigurationseinstellungen sind über das Menü "Admin > Einstellungen" verfügbar. Das Zugreifen auf und Angeben der Konfigurationseinstellungen ist für alle Menüoptionen ähnlich.

Siehe ["Zugreifen auf die Protection Center-Konfigurationseinstellungen"](#) auf Seite 96.

Sie können auf bestimmte Konfigurationseinstellungen direkt im Dialogfeld "Protection Center-Erstes Einrichten" zugreifen. Dieses Dialogfeld wird angezeigt, wenn Sie sich zum ersten Mal bei Protection Center mit dem vordefinierten Protection Center-Administratorkonto (SPC_Admin) einloggen. Im Dialogfeld "Erstes Einrichten" finden Sie Informationen zu Einrichtungsaufgaben, die Sie ausführen müssen, damit Protection Center einsatzbereit ist.

Siehe ["Erstes Einrichten von Protection Center"](#) auf Seite 20.

Die meisten Konfigurationsfunktionen sind nur für den Administrator gedacht. Jedoch kann der Administrator einem Benutzer schreibgeschützten oder Verwaltungszugriff auf bestimmte Optionen des Menüs "Einstellungen" geben, indem er die entsprechenden Berechtigungen im Benutzerkonto festlegt.

Die folgende Tabelle beschreibt die Protection Center-Konfigurationseinstellungen:

Tabelle 9-1 Protection Center-Konfigurationseinstellungen

Element	Beschreibung
Active Directory und LDAP	Ermöglicht das Angeben des Microsoft Active Directory- oder LDAP-Servers, den Protection Center verwendet, um Benutzerkonten zu authentifizieren. Siehe "Verwenden eines Active Directory- oder LDAP-Servers zur Benutzerkontoauthentifizierung" auf Seite 58.
Backup	Ermöglicht das Konfigurieren der Protection Center-Backups. Protection Center verwendet Symantec Backup Exec System Recovery zum Erstellen regelmäßiger Backups. Siehe "Info zu Protection Center-Backup und -Wiederherstellung" auf Seite 83.
Community-Statistik	Hier können Sie das Sammeln und Senden von Diagnoseinformationen und anonymen Nutzungsdaten an das Symantec Global Intelligence Network aktivieren. Diese Daten helfen Symantec, neue Bedrohungen und Trends auf globaler Ebene zu identifizieren. Siehe "Community-Statistik-Einstellungen" auf Seite 96.
Datum/Zeit	Hier können Sie Datum und Uhrzeit von Protection Center festlegen. Siehe "Datums- und Uhrzeiteinstellungen" auf Seite 97.
E-Mail	Geben Sie hier die E-Mail-Adresse ein, an die Protection Center Warnmeldungen senden soll. E-Mail wird auch zum Verteilen von Berichten verwendet. Siehe "E-Mail-Einstellungen" auf Seite 97.

Element	Beschreibung
LiveUpdate	Geben Sie hier an, ob für Protection Center-Software-Updates der LiveUpdate-Server von Symantec oder ein lokaler LiveUpdate-Server verwendet werden soll. Wenn Sie einen lokalen LiveUpdate-Server verwenden, können Sie die entsprechenden Serverdetails angeben. Siehe "Angabe des LiveUpdate-Servers" auf Seite 80.
Nachrichtenprotokollierung	Ermöglicht die Wahl der von Protection Center verwendeten Protokollierungsstufe: normale oder ausführliche Protokollierung. Siehe "Nachrichtenprotokollierungseinstellungen" auf Seite 99.
Netzwerk	Hier können Sie die IPv4- bzw. IPv6-Adresse von Protection Center ändern. Siehe "Netzwerkkonfigurationseinstellungen" auf Seite 100.
Kennwortänderung	Hiermit können Sie Ihr Kennwort jederzeit ändern. Siehe "Ändern des Kennworts für Ihr Benutzerkonto" auf Seite 21.
Produkterkennung	Ermöglicht das Erkennen der von Protection Center unterstützten Produkte, die im Netzwerk installiert sind. Siehe "Erkennen unterstützter Produkte im Netzwerk" auf Seite 34.
Proxy	Ermöglicht das Konfigurieren eines HTTP-Proxy-Servers für Protection Center. Ein Proxy-Server trägt dazu bei, die Sicherheit von Protection Center zu erhöhen. Siehe "Proxy-Server-Einstellungen" auf Seite 100.
Bereinigen	Hiermit können Sie das Bereinigen von älteren Daten in der Protection Center-Datenbank steuern. Sie können die Anzahl der Tage festlegen, für die Daten in der Datenbank gespeichert werden. Siehe "Datenbereinigungseinstellungen" auf Seite 102.
Herunterfahren	Herunterfahren oder Neustarten von Protection Center. Siehe "Herunterfahren oder Neustarten von Protection Center" auf Seite 27.
Support-Diagnosen	Hiermit können Sie Diagnoseninformationen sammeln und für Support-Zwecke an Symantec senden. Siehe "Hilfe vom Symantec-Support" auf Seite 115.
Workflow	Ermöglicht das Konfigurieren von mit Protection Center zu verwendenden Workflows. Siehe "Konfigurieren der Verwaltungseinstellungen für einen Workflow" auf Seite 154. Siehe "Verfügbare Workflows in Protection Center" auf Seite 159.

Zugreifen auf die Protection Center-Konfigurationseinstellungen

Mithilfe der Protection Center-Konfigurationseinstellungen können Sie Protection Center so konfigurieren, dass es in Ihrer Umgebung richtig funktioniert.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Siehe ["Protection Center-Benutzerkontoberechtigungseinstellungen"](#) auf Seite 70.

So greifen Sie auf die Protection Center-Konfigurationseinstellungen zu

- 1 Wählen Sie in Protection Center im Menü "Admin > Einstellungen" die entsprechende Einstellungsoption aus der Liste.
- 2 Geben Sie auf der entsprechenden Konfigurationsseite die entsprechenden Informationen an.
- 3 Klicken Sie auf "Änderungen speichern".

Community-Statistik-Einstellungen

Sie können die Erfassung und das Senden von Diagnosedaten und von anonymen Verwendungsdaten an Symantec aktivieren. Mithilfe dieser Daten, wie zum Beispiel Systemstatistiken und Absturzinformationen, kann Symantec Protection Center-Stabilität nachverfolgen und das Produkt verbessern.

Der Gebrauch dieser Funktion ist optional. Jedoch sollten Sie diese Funktion verwenden, damit Symantec bessere Produktqualität und erweiterten Support gewährleisten kann. Datenerfassung ist standardmäßig aktiviert und wird einmal täglich an Symantec gesendet. Wenn Sie die Datenerfassung deaktivieren, werden die Diagnosedaten nicht mehr gesammelt und an Symantec gesendet. Alle vorherigen Statistiken, die gesammelt wurden, werden bereinigt.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Siehe ["Zugreifen auf die Protection Center-Konfigurationseinstellungen"](#) auf Seite 96.

Tabelle 9-2 Community-Statistik-Einstellungen

Element	Beschreibung
"Community-Statistik aktivieren"	Gibt an, dass die Community-Statistik-Daten gesammelt und an Symantec gesendet werden. Diese Einstellung ist standardmäßig aktiviert. Sie sollten diese Funktion aktivieren, damit Symantec die Daten verwenden kann, um bessere Produktqualität und erweiterten Support gewährleisten zu können.

Element	Beschreibung
Firmenname	Gibt den Namen Ihrer Firma an.

Datums- und Uhrzeiteinstellungen

Sie können Datum und Uhrzeit für die Protection Center-Appliance einstellen.

Siehe "[Protection Center-Konfigurationseinstellungen](#)" auf Seite 93.

Siehe "[Zugreifen auf die Protection Center-Konfigurationseinstellungen](#)" auf Seite 96.

Tabelle 9-3 Datums- und Uhrzeiteinstellungen

Element	Beschreibung
Zeitzone der Appliance	Ermöglicht das Einstellen der Zeitzone fest, in der sich Protection Center befindet. Die Zeitzone wird automatisch erkannt, aber Sie können sie bei Bedarf ändern.
Datum und Uhrzeit der Appliance	Ermöglicht das Einstellen des aktuellen Datums und der aktuellen Uhrzeit für Protection Center.

E-Mail-Einstellungen

Sie können den E-Mail-Server festlegen, den Protection Center zum Versenden von E-Mails verwendet. Protection Center kann Meldungen an Benutzer senden, wie etwa eine Benachrichtigung, wenn ihre neuen Benutzerkonten erstellt sind. Sie können auch die Administrator-E-Mail-Adressen festlegen, an die Protection Center Meldungen sendet. Die E-Mail-Adresse kann eine gültige SMTP-Adresse sein, die von Ihrem SMTP-Server erkannt wird.

Der SMTP-Server, den Sie verwenden, muss SSL-Verbindungen akzeptieren. Zur Gewährleistung der E-Mail-Sicherheit verschlüsselt Protection Center alle Nachrichten.

Siehe "[Protection Center-Konfigurationseinstellungen](#)" auf Seite 93.

Siehe "[Zugreifen auf die Protection Center-Konfigurationseinstellungen](#)" auf Seite 96.

Protection Center sendet eine E-Mail, wenn ein dringendes Problem auftritt, das möglicherweise Aufmerksamkeit erfordert. Diese E-Mails tragen dazu bei, dass Protection Center problemlos funktioniert.

Geben Sie eine E-Mail-Adresse und gültige SMTP-Serverinformationen an, um E-Mails mit den folgenden Informationen zu erhalten:

- Benachrichtigungen über erfolgreich verteilte Berichte
- Automatische Aktionen, die ausgeführt wurden
- Systemprüfungen
- Benachrichtigungen von unterstützten Produkten
- Benachrichtigungen zu Problemen mit Protection Center

Diese E-Mails helfen Ihnen, Protection Center-Aktivitäten zu überwachen und zu verwalten.

Tabelle 9-4 SMTP-Servereinstellungen

Element	Beschreibung
Server	Ermöglicht die Angabe des Hostnamen oder die IP-Adresse des SMTP-Servers, den Protection Center zum Versenden von E-Mails verwendet. Protection Center verwendet diesen Server zum Versenden von E-Mails, um den Administrator über alle dringenden Probleme zu informieren und regelmäßige Berichte zu verteilen.
Port	Ermöglicht das Festlegen des Ports, über den auf den SMTP-Server zugegriffen wird.
Benutzername	Ermöglicht die Eingabe des Benutzernamen eines Kontos mit Zugriffsrechten für den SMTP-Server.
Kennwort	Ermöglicht die Eingabe des Kennworts für das Benutzerkonto.

Tabelle 9-5 Administrator-E-Mail-Einstellungen

Element	Beschreibung
Absenderadresse	Ermöglicht das Festlegen der angezeigten E-Mail-Adresse als E-Mail-Absender in allen E-Mails, die von Protection Center gesendet werden.
Absendername	Ermöglicht das Festlegen der E-Mail-Absendernamen. Dieser Name wird als E-Mail-Absender (Von:) in allen E-Mails angezeigt, die Protection Center sendet. Dieser Name sollte der E-Mail-Adresse entsprechen, die Sie angeben haben.
Empfängeradresse	Ermöglicht das Festlegen der E-Mail-Adresse, an die Protection Center administrative E-Mails sendet. Die regelmäßigen Berichte werden nicht an diese E-Mail-Adresse gesendet. Die E-Mail-Adressen für Berichte werden für jeden Bericht festgelegt. Siehe " Berichtsverteilungseinstellungen " auf Seite 143.
Verfügbarkeitswarnmeldungen senden	Ermöglicht, das Senden von generierten Systembenachrichtigungen an den Administrator zu aktivieren.

Element	Beschreibung
Test-E-Mail senden	Ermöglicht das Prüfen des E-Mail-Servers und der Adresseinstellungen, indem eine E-Mail unter Verwendung der aktuellen Einstellungen gesendet wird.

Nachrichtenprotokollierungseinstellungen

Protection Center behält ein Nachrichtenprotokoll bei. Sie können die Stufe der Nachrichtenprotokollierung steuern, die Protection Center durchführt: normale oder ausführliche Protokollierung. Symantec empfiehlt, dass Sie die normale Protokollierungsoption für tägliche Protokollierung auswählen. Sie können zur ausführlichen Protokollierungsoption wechseln, um die Fehlerbehebung eines technischen Problems zu erleichtern. Nachdem das Problem gelöst ist, setzen Sie es zurück auf die normalen Protokollierungsoption.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Siehe ["Zugreifen auf die Protection Center-Konfigurationseinstellungen"](#) auf Seite 96.

Sie können die Systemprotokollprotokolldateien über den Systemprotokolle-Bericht anzeigen. Um Zugriff auf den Systemprotokolle-Bericht zu erhalten, benötigen Sie eine Systemprotokollberechtigung für Ihr Benutzerkonto.

Siehe ["Anzeigen eines Berichts"](#) auf Seite 136.

Standardmäßig werden die Protokolldateien 30 Tage lang gespeichert. Jedoch können Sie die Sperrfrist gemäß dem Umfang Ihrer Daten und Ihrer bestimmten Aufbewahrungnotwendigkeiten durch die Datenbereinigungseinstellungen ändern.

Siehe ["Datenbereinigungseinstellungen"](#) auf Seite 102.

Tabelle 9-6 Nachrichtenprotokollierungseinstellungen

Element	Beschreibung
Normal	Protokolliert nur den Fehler, die Warnung und die Informationsmeldungen.
Ausführlich	Protokolliert den Fehler, die Warnung und die Informationsmeldungen zusammen mit den zusätzlichen Meldungen, die für Debuggingzwecke verwendet werden können.

Netzwerkkonfigurationseinstellungen

Sie können die Netzwerkeinstellungen konfigurieren, die Protection Center verwendet. Sie können eine IPv4-Adresse und eine IPv6-Adresse sowie DNS-Einstellungen für beide konfigurieren. Für Protection Center muss eine IPv4-Adresse konfiguriert sein. Die IPv6-Adresse ist optional. Sie müssen eine statische IP-Adresse konfigurieren. Protection Center unterstützt keine dynamischen IP-Adressen.

Sie können die Netzwerkeinstellungen über die Protection Center-Schnittstelle oder über die Protection Center-Systemsteuerung konfigurieren.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Siehe ["Zugreifen auf die Protection Center-Konfigurationseinstellungen"](#) auf Seite 96.

Siehe ["Protection Center-Systemsteuerungsoptionen"](#) auf Seite 105.

Siehe ["Zugreifen auf die Protection Center-Systemsteuerung"](#) auf Seite 107.

Siehe ["Netzwerkeinstellungen angeben"](#) auf Seite 109.

Tabelle 9-7 IP-Adresseinstellungen

Element	Beschreibung
"IP-Adresse der Appliance"	Gibt die IP-Adresse der Protection Center-Appliance an.
Subnetzmaske	(Nur IPv4-Adressen) Gibt die Subnetzmaske an.
"Länge des Subnetzpräfix"	(Nur IPv6-Adressen) Gibt die Länge des Subnetzpräfix an.
Standard-Gateway	Gibt das Standard-Gateway an.

Tabelle 9-8 DNS-Einstellungen

Element	Beschreibung
Primärserver	Gibt die DNS-Adresse des Primärservers an.
Alternativer Server	Gibt die DNS-Adresse des Sekundärservers an.

Proxy-Server-Einstellungen

Sie können einen HTTP-Proxy-Server für Protection Center festlegen. Das Verwenden eines Proxy-Servers kann die Sicherheit von Protection Center erhöhen, da der Proxy-Server direkten Zugriff auf Protection Center verhindert. Befindet sich Protection Center beispielsweise innerhalb der Firewall Ihres Unternehmens,

gewährleistet das Einrichten eines Proxy-Servers einen sicheren Weg durch die Firewall, ohne die Sicherheit von Protection Center zu gefährden. Das Verwenden eines Proxy-Servers hilft Protection Center, auf sicherere Weise Patches oder Updates von externen Websites herunterzuladen.

Protection Center ist standardmäßig konfiguriert, keinen Proxy-Server zu verwenden. Das Verwenden eines Proxy-Servers hängt davon ab, wie Ihre Netzwerkumgebung konfiguriert ist.

Siehe "[Protection Center-Konfigurationseinstellungen](#)" auf Seite 93.

Siehe "[Zugreifen auf die Protection Center-Konfigurationseinstellungen](#)" auf Seite 96.

Tabelle 9-9 HTTP-Proxy-Servereinstellungen

Element	Beschreibung
Keinen HTTP-Proxy-Server verwenden	Gibt an, dass Protection Center keinen Proxy-Server für HTTP-Verbindungen verwendet.
Angegebene HTTP-Proxy-Servereinstellungen verwenden	Gibt an, dass Protection Center einen HTTP-Proxy-Server verwendet.
HTTP-Proxy-Server	Gibt den Hostnamen oder die IP-Adresse des HTTP-Proxy-Servers an, den Protection Center verwenden soll.
Proxy-Server-Port	Gibt den Port an, mit dem auf den HTTP-Proxy-Server zugegriffen wird.
HTTP-Proxy-Serverbenutzername	Gibt den Benutzernamen eines Kontos an, das die Berechtigung hat, auf den HTTP-Proxy-Server zuzugreifen. Diese Einstellung ist optional. Sie muss nur angegeben werden, wenn der Proxy-Server Identifikationsdaten erfordert.
HTTP-Proxy-Serverkennwort	Gibt das Kennwort eines Benutzerkontos an, das die Berechtigung hat, auf den HTTP-Proxy-Server zuzugreifen. Diese Einstellung ist optional. Sie muss nur angegeben werden, wenn der Proxy-Server Identifikationsdaten erfordert.

Element	Beschreibung
HTTP-Einstellungen testen	Testet die HTTP-Proxy-Servereinstellungen. Protection Center verwendet die angegebenen Einstellungen, um eine Verbindung zu einer externen Website herzustellen. Sie müssen die Konfigurationseinstellungen speichern, bevor Sie die HTTP-Proxy-Einstellungen testen können. Wird während des Tests der Einstellungen eine Fehlermeldung angezeigt, stellen Sie sicher, dass Ihre Authentifizierungsdaten richtig sind und dass Ihr Proxy-Server läuft. Sie sollten auch sicherstellen, dass keine allgemeinen Netzwerkfehler vorliegen.

Datenbereinigungseinstellungen

Sie können steuern, wie lange Protection Center-Daten aufbewahrt werden, bevor sie von der Protection Center-Datenbank entfernt werden. Der Bereinigungsvorgang betrifft keine Daten von integrierten Produkten.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Siehe ["Zugreifen auf die Protection Center-Konfigurationseinstellungen"](#) auf Seite 96.

Protection Center bereinigt die folgenden Daten:

- Ereignisübersichtsdaten, die Protection Center basierend auf der Verarbeitung kommender Ereignissen generiert
- Ereignisdaten, die in den Archiven gespeichert werden
- Diagnosenhauptdumps
- Protokolldateien

Protection Center zeigt den gesamten Speicherplatz für die folgenden Datentypen an: Benachrichtigungen, Rohdatenereignisse, Übersichtsdaten, Support-Dateien und andere Daten. Mithilfe dieser Informationen können Sie die von Protection Center verwendete Menge an Speicherplatz nachvollziehen.

Tabelle 9-10 Datenbereinigungseinstellungen

Element	Beschreibung
"Daten aufbewahren für (Tage)"	Ermöglicht Ihnen, die maximale Zeitdauer einzustellen, für die Daten in der Protection Center-Datenbank gespeichert werden sollen. Die Sperrfrist ist in Tagen festgelegt.

Element	Beschreibung
"Uhrzeit der täglichen Datenbereinigung"	Ermöglicht es Ihnen, die Uhrzeit einzustellen, zu der der Bereinigungsprozess beginnen soll. Symantec empfiehlt dass Sie den Bereinigungsprozess außerhalb von Spitzenzeiten durchführen. Datenbereinigung außerhalb von Spitzenzeiten verhindert übermäßige Last in Protection Center während Spitzenzeiten.
"Jetzt bereinigen"	Führt den Bereinigungsprozess sofort aus. Alle Daten, die älter ist, als die aktuelle Einstellung "Daten aufbewahren für (Tage):" werden aus der Datenbank entfernt. Der Bereinigungszeitplan ist nicht betroffen. Wenn der Wert im Feld "Daten aufbewahren für (Tage):" nicht gespeichert worden ist, verwendet Protection Center den zuletzt im Bereinigungsprozess gespeicherten Wert.

Die Protection Center-Systemsteuerung

In diesem Kapitel werden folgende Themen behandelt:

- [Protection Center-Systemsteuerungsoptionen](#)
- [Zugreifen auf die Protection Center-Systemsteuerung](#)
- [Manuelles Aktualisieren der Protection Center-Software](#)
- [Ändern des Kennworts für das SPC_Admin-Konto](#)
- [Netzwerkeinstellungen angeben](#)
- [Windows-Betriebssystem aktivieren](#)

Protection Center-Systemsteuerungsoptionen

Die Protection Center-Systemsteuerung ist die Benutzeroberfläche der Protection Center-Appliance, die dem Desktop eines Windows-Computers entspricht. In der Systemsteuerung können Sie einige wesentliche Konfigurationsaufgaben ausführen. Einige der Aufgaben, die Sie über die Systemsteuerung ausführen können, sind auch in der Protection Center-Schnittstelle verfügbar. Beispielsweise können Sie an beiden Stellen die Appliance-Software aktualisieren, das Administratorkennwort ändern und die Appliance-Netzwerkeinstellungen angeben. Bestimmte Aufgaben, wie zum Beispiel das Aktivieren von Windows, können jedoch nur über die Systemsteuerung ausgeführt werden.

Möglicherweise müssen Sie Änderungen an Ihrer Protection Center-Installation vornehmen, um sie an die Bedürfnisse Ihres Unternehmens anzupassen. Weitere Informationen finden Sie im Handbuch zur Größenaufteilung und Skalierbarkeit von Symantec Protection Center.

Die Systemsteuerung ist nicht dasselbe wie die Protection Center-Schnittstelle. Die Protection Center-Schnittstelle ist eine browserbasierte Benutzeroberfläche, mit deren Hilfe sich Protection Center-Benutzer von Remote-Computern aus bei Protection Center einloggen können.

Bevor Sie auf die Systemsteuerung zugreifen können, müssen Sie einen Monitor direkt mit der Protection Center-Appliance verbinden. Alternativ können Sie eine virtuelle Konsole verwenden, wenn innerhalb Ihrer virtuellen Umgebung eine zur Verfügung gestellt wird.

Hinweis: Nur das Protection Center-Administratorkonto (SPC_Admin) kann auf die Protection Center-Systemsteuerung zugreifen.

Siehe ["Info zum SPC_Admin-Konto"](#) auf Seite 57.

Siehe ["Protection Center-Konfigurationseinstellungen"](#) auf Seite 93.

Tabelle 10-1 Protection Center-Systemsteuerungsoptionen

Option	Beschreibung
Protection Center-Update	Ermöglicht das Aktualisieren von Protection Center durch manuelles Ausführen einer Protection Center-Update-Datei. Siehe "Manuelles Aktualisieren der Protection Center-Software" auf Seite 107.
Administratorkennwort	Hiermit können Sie das Kennwort für das vordefinierte Protection Center-Administratorkonto (SPC_Admin) ändern. Siehe "Ändern des Kennworts für das SPC_Admin-Konto" auf Seite 108.
IPv4-Netzwerkeinstellungen	Hier können Sie die IPv4-Netzwerkeinstellungen angeben, die Protection Center verwendet. Siehe "Netzwerkeinstellungen angeben" auf Seite 109.
IPv6-Netzwerkeinstellungen	Hier können Sie die IPv6-Netzwerkeinstellungen angeben, die Protection Center verwendet. Siehe "Netzwerkeinstellungen angeben" auf Seite 109.
Windows-Aktivierung	Hiermit können Sie Kopie von Microsoft Windows aktivieren, die Protection Center verwendet. Siehe "Windows-Betriebssystem aktivieren" auf Seite 111.
Sprache	Hier können Sie die Sprache auswählen, die für die Protection Center-Systemsteuerung verwendet werden soll.
Rote Schaltfläche	Die rote Schaltfläche mit dem Kreis und der vertikalen Linie dient zum Herunterfahren von Protection Center.

Option	Beschreibung
Pfeilschaltfläche	Hiermit können Sie sich ausloggen sowie die Protection Center-Appliance herunterfahren oder neu starten. Die Pfeilschaltfläche öffnet ein Kontextmenü mit Optionen zum Ausloggen sowie zum Neustarten oder Herunterfahren von Protection Center. Diese Funktionalität entspricht dem Drücken von Strg+Alt+Entf in der Protection Center-Appliance.

Zugreifen auf die Protection Center-Systemsteuerung

Die Protection Center-Systemsteuerung ist die Appliance-Benutzeroberfläche, die dem Desktop eines Windows-Computers entspricht. Bevor Sie auf die Systemsteuerung zugreifen können, müssen Sie einen Monitor direkt mit der Protection Center-Appliance verbinden. Alternativ können Sie eine virtuelle Konsole verwenden, wenn innerhalb Ihrer virtuellen Umgebung eine zur Verfügung gestellt wird.

Siehe ["Protection Center-Systemsteuerungsoptionen"](#) auf Seite 105.

Nur das Protection Center-Administratorkonto (SPC_Admin) kann auf die Protection Center-Systemsteuerung zugreifen.

Siehe ["Info zum SPC_Admin-Konto"](#) auf Seite 57.

Siehe ["Ändern des Kennworts für das SPC_Admin-Konto"](#) auf Seite 108.

So greifen Sie auf die Protection Center-Systemsteuerung zu

- 1 Verbinden Sie einen Monitor mit der Protection Center-Appliance oder verwenden Sie eine Konsole, die von Ihrer virtuellen Umgebung zur Verfügung gestellt wird.
- 2 Drücken Sie Strg+Alt+Entf.
- 3 Geben Sie im Login-Bildschirm die Identifikationsdaten des Protection Center-Administratorkontos (SPC_Admin) ein.

Manuelles Aktualisieren der Protection Center-Software

Standardmäßig verwendet Protection Center LiveUpdate, seine Softwarekomponenten automatisch auf dem neuesten Stand zu halten. Außerdem verwendet Protection Center LiveUpdate, um die Informationen zu aktualisieren, die Protection Center für das Zusammenwirken mit unterstützten Produkten benötigt.

Siehe "[Verwalten von Protection Center-Softwareupdates](#)" auf Seite 78.

Siehe "[Weitere Informationen zu Protection Center](#)" auf Seite 15.

Wenn Sie nicht die automatische Aktualisierungsfunktion von Protection Center verwenden, können Sie die Protection Center-Software manuell aktualisieren. Sie müssen möglicherweise manuelle Aktualisierungen verwenden, wenn Protection Center keinen Zugang zum Internet hat. Außerdem können Sie manuelle Aktualisierungen ausführen, wenn Sie eine Aktualisierung sofort benötigen und nicht auf den automatischen Mechanismus warten möchten.

Siehe "[Protection Center-Systemsteuerungsoptionen](#)" auf Seite 105.

So aktualisieren Sie die Protection Center-Software manuell

- 1 Wechseln Sie auf einem Computer, der Zugang zum Internet hat, zu folgender URL:

<http://go.symantec.com/protection-center>

- 2 Wählen Sie auf der Protection Center-Webseite "Verwenden" und dann "Product Updates" aus.
- 3 Suchen Sie die entsprechenden Update-Dateien und laden Sie sie herunter.
- 4 Speichern Sie die Dateien auf entsprechenden Speichermedien (USB-Laufwerk, DVD oder CD), die die Protection Center-Appliance lesen kann.
Wählen Sie keine Netzlaufwerke, Websites oder FTP-Adressen.
- 5 Loggen Sie sich bei Protection Center ein.

Siehe "[Zugreifen auf die Protection Center-Systemsteuerung](#)" auf Seite 107.

- 6 Klicken Sie in der Protection Center-Systemsteuerung unter "Manuelles Protection Center-Update" auf "Protection Center-Update installieren".
- 7 Klicken Sie im Dialogfeld "Protection Center-Update installieren" klicken Sie auf "Durchsuchen" und wählen Sie dann die Aktualisierungsdatei aus, die Sie installieren möchten.
- 8 Klicken Sie auf "Ausführen".

Die nächsten Schritte hängen davon ab, welches Aktualisierungsskript ausgeführt wird. In einigen Fällen werden Sie aufgefordert, Protection Center neu zu starten, oder müssen weitere Aktionen ausführen.

Ändern des Kennworts für das SPC_Admin-Konto

Sie können das Kennwort für das SPC_Admin-Konto über die Protection Center-Systemsteuerung ändern.

Siehe ["Info zum SPC_Admin-Konto"](#) auf Seite 57.

Siehe ["Protection Center-Systemsteuerungsoptionen"](#) auf Seite 105.

So ändern Sie das Kennwort für das SPC_Admin-Konto

- 1 Loggen Sie sich bei Protection Center ein.

Siehe ["Zugreifen auf die Protection Center-Systemsteuerung"](#) auf Seite 107.

- 2 Klicken Sie in der Protection Center-Systemsteuerung unter "Administratorkennwort" auf "Kennwort ändern".

- 3 Geben Sie im Dialogfeld "Kennwort ändern" die folgenden Details ein.

Aktuelles Kennwort	Das aktuelle Kennwort für das SPC_Admin-Konto.
Neues Kennwort	Das neue Kennwort für das SPC_Admin-Konto. Das Kennwort muss aus mindestens acht Zeichen bestehen und mindestens drei der folgenden Angaben enthalten: ■ Alphabetische Großbuchstaben (A bis Z) ■ Alphabetische Unicode-Zeichen, die weder Großbuchstaben (A bis Z) noch Kleinbuchstaben (a bis z) sind ■ Numerisches Zeichen (0 bis 9) ■ Nicht alphanumerische Zeichen (~!@#\$\$%^&* _-+=`\'()\{\}\[\];:~!@#\$.?/)
Kennwort bestätigen	Das neue Kennwort für das SPC_Admin-Konto.

- 4 Klicken Sie auf "OK".

Netzwerkeinstellungen angeben

In einigen Szenarien wären Sie möglicherweise nicht in der Lage, im Netzwerk auf Protection Center zuzugreifen. Beispielsweise könnte aufgrund der Konfiguration von Protection Center über die Protection Center-Schnittstelle möglicherweise eine falsche IP-Adresse, Subnetzmaske oder falsche Gateway-Informationen angegeben werden. Durch die Systemsteuerungsfunktionalität wird gewährleistet, dass solche Netzwerkkonfigurationsprobleme behoben werden können.

Sie können die Netzwerkeinstellungen konfigurieren, die Protection Center verwendet. Sie können eine IPv4-Adresse und eine IPv6-Adresse konfigurieren. Für Protection Center muss eine IPv4-Adresse konfiguriert sein. Die IPv6-Adresse

ist optional. Sie müssen eine statische IP-Adresse konfigurieren. Protection Center enthält keine Option zur Konfiguration einer DHCP-Adresse.

Siehe "[Protection Center-Systemsteuerungsoptionen](#)" auf Seite 105.

Sie können die Netzwerkeinstellungen auch über die Protection Center-Schnittstelle konfigurieren.

Siehe "[Netzwerkkonfigurationseinstellungen](#)" auf Seite 100.

So geben Sie Netzwerkeinstellungen an

- 1 Loggen Sie sich bei Protection Center ein.

Siehe "[Zugreifen auf die Protection Center-Systemsteuerung](#)" auf Seite 107.

- 2 Führen Sie in der Protection Center-Systemsteuerung einen der folgenden Schritte durch:

So geben Sie die IPv4-Netzwerkeinstellungen an	Unter "IPv4-Netzwerkeinstellungen" klicken Sie auf "IPv4-Netzwerkeinstellungen eingeben".
--	---

So geben Sie die IPv6-Netzwerkeinstellungen an	Unter "IPv6-Netzwerkeinstellungen" klicken Sie auf "IPv6-Netzwerkeinstellungen eingeben".
--	---

- 3 Aktivieren Sie im Dialogfeld "IPv4-Netzwerkeinstellungen eingeben" bzw. im Dialogfeld "IPv6-Netzwerkeinstellungen eingeben" eine der folgenden Optionen:

IPv6 nicht konfigurieren	Für Protection Center wird keine IPv6-Adresse konfiguriert. Alle vorhandenen Konfigurationseinstellungen werden deaktiviert. Diese Option ist nur im Dialogfeld "IPv6-Netzwerkeinstellungen eingeben" verfügbar.
Folgendes verwenden	Eine IPv4- oder IPv6-Adresse (je nachdem, welche geeignet ist) wird für Protection Center unter Verwendung der angegebenen Einstellungen konfiguriert.

- 4 Geben Sie die entsprechenden IP-Adressen- und DNS-Einstellungen ein.
- 5 Klicken Sie auf "OK".

Windows-Betriebssystem aktivieren

Sie können Windows aktivieren, indem Sie einen Produktschlüssel eingeben oder den Lizenzservernamen angeben. Microsoft erfordert, dass Sie ein Windows-Betriebssystem aktivieren, damit es richtig lizenziert werden kann. Sie können auch den Windows Update-Server-Speicherort konfigurieren, den Protection Center zur Verwaltung von Sicherheitsupdates für Windows verwendet.

Hinweis: Wenn Sie Windows während der Erstellung der Appliance aktiviert haben, müssen Sie keine weiteren Konfigurationsschritte durchführen. Sie sollten diese Funktion nur dann verwenden, wenn Sie die Windows-Einstellungen ändern möchten.

Wenn der Lizenzserver nicht den Standard-Port verwendet, müssen Sie den richtigen Port angeben. Sie müssen einen Doppelpunkt (:) und die Port-Nummer an das Ende des Servernamens anfügen. Beispiel: **kms.server.com:6000** oder **192.196.15.25:6000**.

Siehe "[Protection Center-Systemsteuerungsoptionen](#)" auf Seite 105.

So aktivieren Sie das Windows-Betriebssystem

- 1 Loggen Sie sich bei Protection Center ein.

Siehe "[Zugreifen auf die Protection Center-Systemsteuerung](#)" auf Seite 107.

- 2 Klicken Sie in der Protection Center-Systemsteuerung unter "Windows-Aktivierung und -Einstellungen" auf "Windows-Einstellungen ändern".

Ein gelbes Symbol links von dieser Option mit dem Text "Windows ist nicht aktiviert" weist darauf hin, dass Windows nicht aktiviert wurde.

Wenn Windows bereits aktiviert ist, wird kein Symbol angezeigt. Außerdem wird "Windows ist aktiviert" sowie die entsprechende Produkt-ID angezeigt.

- 3** Führen Sie im Dialogfeld "Windows-Einstellungen ändern" unter "Aktivierung" einen der folgenden Schritte durch:

So verwenden Sie einen Produktschlüssel	Klicken Sie auf "Windows-Produktschlüssel" und geben Sie dann den entsprechenden Produktschlüssel ein. Sie erhalten den notwendigen Produktschlüssel von Microsoft.
So verwenden Sie einen Lizenzserver	Klicken Sie auf "Windows-Lizenzserver" und geben Sie dann den entsprechenden Lizenzservernamen ein. Sie erhalten die Adresse des Schlüsselverwaltungsservers von Ihrem Systemadministrator.

- 4** Geben Sie unter "Updates" den gewünschten Windows Update Server an:

So verwenden Sie die Update Server von Microsoft	Klicken Sie auf "Windows Update Server von Microsoft aus dem Internet verwenden".
So verwenden Sie einen lokalen Update Server	Klicken Sie auf "Geben Sie eine URL für den lokal beibehaltenen Windows Update Server an" und geben Sie dann die entsprechende URL ein. Sie erhalten die Adresse des lokalen Windows Update Servers von Ihrem Systemadministrator.

- 5** Klicken Sie auf "OK".

Wenn Windows erfolgreich aktiviert wurde, werden das gelbe Symbol und die Nachricht "Windows ist nicht aktiviert" durch die entsprechende Produkt-ID und die Nachricht "Windows ist aktiviert" ersetzt.

Wenn die Windows-Aktivierung aufgrund eines ungültigen Produktschlüssels oder einer falschen Schlüsselverwaltungsserveradresse fehlschlägt, wird das Standard-Dialogfeld von Microsoft für Aktivierungsfehler angezeigt. Sie müssen die Fehlermeldung lesen und die entsprechenden Schritte unternehmen, um den Fehler zu beheben.

Sie müssen keinen Neustart durchführen. Wird ein Produktschlüssel verwendet, wird er zur Prüfung an Microsoft gesendet. Wenn ein Schlüsselverwaltungsserver verwendet wird, kommuniziert der Schlüsselverwaltungsserver bei Aktivierung von Windows mit der Protection Center-Appliance.

Hilfe bei Problemen mit Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Ressourcen zur Problembehebung in Protection Center](#)
- [Hilfe vom Symantec-Support](#)
- [Symantec-Support-Diagnoseoptionen](#)
- [Sammeln von Protection Center-Diagnosedaten](#)
- [Supportanfrageneinstellungen](#)
- [Speichern einer Diagnosedatei](#)
- [Senden einer Diagnosedatei an den Symantec-Support](#)

Ressourcen zur Problembehebung in Protection Center

Wenn Sie auf ein Problem mit Protection Center stoßen, sehen Sie zunächst im *Protection Center-Benutzerhandbuch* oder in der Hilfe nach. Wenn Sie die benötigten Informationen nicht finden können, stehen weitere Ressourcen zur Verfügung. Die folgende Tabelle zeigt, welche Ressourcen verfügbar sind für welche Probleme sie sich jeweils eignen.

Tabelle 11-1 Ressourcen zur Problembehebung in Protection Center

Ressource	Beschreibung
Versionshinweise zu Protection Center	In den Protection Center-Versionshinweisen finden Sie die neuesten Informationen über Probleme und Abhilfemaßnahmen. Die Versionshinweise zu Protection Center werden laufend aktualisiert, während der Symantec-Support und andere Produktexperten neue Probleme analysieren und Lösungen anbieten. Versionshinweise sind geeignet, wenn Sie überprüfen müssen, ob Sie Informationen zu bestimmten Funktionen oder Aufgaben benötigen. Wenn eine Funktion in Protection Center nicht wie erwartet oder wie in der Benutzerdokumentation beschrieben funktioniert, finden Sie möglicherweise eine aktuelle Beschreibung in den Versionshinweisen. Sie können auf die Versionshinweise von der Protection Center-Seite auf der Symantec-Website zugreifen. Die Protection Center-Seite befindet sich unter folgender URL: http://go.symantec.com/protection-center
SymWISE	SymWISE ist die Supportdatenbank von Symantec. Hier können Sie nach speziellen Informationen suchen. Anders als die Benutzerdokumentation enthält die Supportdatenbank Artikel mit Antworten auf ganz bestimmte Fragen und Probleme. Die Supportdatenbank ist eine gute Ressource, wenn ein Problem auftritt und Sie vermuten, dass dasselbe Problem auch bei anderen Benutzern aufgetreten ist oder diese die Lösung kennen. Die Supportdatenbank ist ebenfalls die richtige Adresse, wenn Sie Hilfe in einer Situation benötigen, die zu speziell ist, um in der Dokumentation behandelt zu werden. Sie können auf SymWISE unter folgender URL zugreifen: http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Bericht "Systemprotokolle"	Der Bericht "Systemprotokolle" enthält Details zu den Aktivitäten innerhalb von Protection Center. Diese Informationen können Ihnen bei der Diagnose aufgetretener Probleme helfen. Auf diesen Bericht wird über die Registerkarte "Berichte" in Protection Center zugegriffen. Der Bericht "Systemprotokolle" ist eine gute Ressource, wenn Sie Informationen zu Ereignissen abrufen möchten, die in Ihrem System aufgetreten sind. Informationen in den Protokollen können Ihnen helfen, Ihr Problem zu identifizieren.

Ressource	Beschreibung
SymConnect-Foren	In den SymConnect-Foren können Sie nach Antworten suchen und Fragen stellen. Produktexperten und andere Benutzer, die möglicherweise auf ähnliche Probleme gestoßen sind und diese gelöst haben, überwachen diese Foren und geben Beiträge ein. Die SymConnect-Foren sind eine gute Ressource, wenn Sie Ihre speziellen Fragen einer Community von Protection Center-Benutzern stellen möchten. Sie können auf SymConnect unter folgender URL zugreifen: http://www.symantec.com/connect/
Symantec Support	Das Symantec-Support-Team hat umfangreiche Erfahrung mit Protection Center und kann Ihnen bei allen Problemen helfen, die möglicherweise bei Ihnen auftreten. Bei der Zusammenarbeit mit dem Symantec-Support müssen Sie möglicherweise eine Diagnosedatei vorbereiten und einsenden, um dem Symantec-Support die Diagnose Ihres Problems zu erleichtern. Der Symantec-Support ist eine gute Ressource, wenn Sie Ihr Problem nicht auf andere Weise lösen können und direkt mit einem Experten mit umfassenden Kenntnissen des Produkts sprechen müssen. Siehe "Hilfe vom Symantec-Support" auf Seite 115.

Hilfe vom Symantec-Support

Wenn Sie vom Symantec-Support Unterstützung bei einem Protection Center-Problem benötigen, bittet der Support Sie möglicherweise, Diagnosedaten zu sammeln, die bei der Lösung des Problems helfen können. Wenn Sie die Diagnosedatensammlung ausführen, sendet Protection Center eine verschlüsselte Diagnosedatei an den Symantec-Support.

Siehe "[Ressourcen zur Problembehebung in Protection Center](#)" auf Seite 113.

Siehe "[Symantec-Support-Diagnoseoptionen](#)" auf Seite 116.

Siehe "[Supportanfrageneinstellungen](#)" auf Seite 120.

Tabelle 11-2 Prozess für Hilfe vom Symantec-Support

Schritt	Aktion	Beschreibung
Schritt 1	Stellen Sie sicher, dass die ausführliche Protokollierung konfiguriert ist.	Die Protection Center-Nachrichtenprotokollierung muss möglichst viele Informationen sammeln, die beim Diagnostizieren des Problems helfen können. Sobald Sie ein Problem mit Protection Center feststellen, sollten Sie die ausführliche Protokollierung konfigurieren. Siehe "Nachrichtenprotokollierungseinstellungen" auf Seite 99.

Schritt	Aktion	Beschreibung
Schritt 2	Bitten Sie den Symantec-Support um Hilfe.	Starten Sie in Kontakt mit dem Symantec-Support den Diagnoseprozess. Der Symantec-Support bittet Sie, die Protection Center-Diagnoseinformationen zu sammeln. Das Support-Team gibt Ihnen eine eindeutige Kundenservice-Fall-ID für Ihr Problem.
Schritt 3	Erstellen Sie die entsprechende Supportanfrage.	Öffnen Sie in Protection Center die Symantec-Support-Diagnoseseite. Auf dieser Seite können Sie eine Supportanfrage erstellen und so konfigurieren, dass eine verschlüsselte Diagnosedatei an den Symantec-Support gesendet wird. Sie müssen die entsprechenden Details angeben: Ihre Kundenservice-Fall-ID, die zu verwendende Konfigurationsdatei und die Daten für die Übertragung der Diagnosedatei. Siehe " Sammeln von Protection Center-Diagnosedaten " auf Seite 118.
Schritt 4	(Optional) Führen Sie die Diagnosedatensammlung erneut aus.	Bei Bedarf, können Sie die Einstellungen für Ihre Supportanfrage ändern und die Diagnosedatensammlung wiederholen. Einige Probleme erfordern möglicherweise, dass Sie mehrmals Diagnosedaten sammeln, bis das Problem gelöst werden kann. Siehe " Sammeln von Protection Center-Diagnosedaten " auf Seite 118.
Schritt 5	Senden Sie die Diagnoseergebnisse an den Symantec-Support.	Sie können die Diagnoseergebnisdatei aus Protection Center herunterladen und auf Ihrem lokalen Laufwerk speichern. Anschließend können Sie die Diagnoseergebnisdatei in eine E-Mail anhängen und an den Symantec-Support senden. Alternativ können Sie die Datei per FTP übertragen. Siehe " Speichern einer Diagnosedatei " auf Seite 122. Siehe " Senden einer Diagnosedatei an den Symantec-Support " auf Seite 123.

Symantec-Support-Diagnoseoptionen

In Protection Center können Sie für Fehlerbehebungszwecke eine verschlüsselte Diagnosedatei erstellen und an den Symantec-Support senden. Außerdem werden Einzelheiten der aktuellen Supportanfrage angezeigt: die Kundenservice-Fall-ID, die Dateübertragungsdetails und die Ergebnisse der Diagnosedatensammlung.

Hinweis: Die Protection Center-Nachrichtenprotokollierung muss möglichst viele Informationen sammeln, die beim Diagnostizieren des Problems helfen können. Sie müssen die ausführliche Protokollierung konfigurieren, bevor Sie versuchen, Diagnosedaten zu sammeln.

Siehe "[Nachrichtenprotokollierungseinstellungen](#)" auf Seite 99.

Wenn Sie die Protection Center-Diagnosedaten sammeln müssen, liefert der Symantec-Support die Informationen, die Sie benötigen, um den entsprechenden Kundenservice-Fall zu erstellen. Zu diesen Informationen gehören die Kundenservice-Fall-ID, die entsprechende Konfigurationsdatei und die FTP-Dateiübertragungsinformationen.

Siehe "[Hilfe vom Symantec-Support](#)" auf Seite 115.

Tabelle 11-3 Symantec-Support-Diagnoseoptionen

Option	Beschreibung
Neue Support-Anfrage erstellen	Ermöglicht das Erstellen eines neuen Kundenservice-Falls. Sie müssen die entsprechenden Details im Dialogfeld "Neue Support-Anfrage starten" angeben. Siehe "Sammeln von Protection Center-Diagnosedaten" auf Seite 118. Siehe "Supportanfrageneinstellungen" auf Seite 120.
Diagnose erneut ausführen	Hiermit können Sie die Supportanfrageneinstellungen ändern und die Diagnosedatensammlung wiederholen. Einige Probleme erfordern möglicherweise, dass Sie mehrmals Diagnosedaten sammeln, bis das Problem gelöst werden kann. Siehe "Sammeln von Protection Center-Diagnosedaten" auf Seite 118. Siehe "Supportanfrageneinstellungen" auf Seite 120.
Diagnosedatei speichern	Hiermit können Sie die Diagnoseergebnisdatei aus Protection Center herunterladen und auf Ihrem lokalen Laufwerk speichern. Siehe "Speichern einer Diagnosedatei" auf Seite 122.
Diagnosen an Support senden	Hiermit können Sie Diagnoseergebnisse manuell an den Symantec-Support senden. Wenn Sie in der Supportanfrage keine FTP-Übertragungsdetails angeben, wird die Diagnoseergebnisdatei nicht zum Symantec-Support übertragen. Beim Sammeln der Diagnosedaten wird die Diagnoseergebnisdatei in Protection Center gespeichert. Mit dieser Option können Sie die Diagnoseergebnisse später zum Symantec-Support übertragen. Siehe "Senden einer Diagnosedatei an den Symantec-Support" auf Seite 123.

Tabelle 11-4 Symantec-Support-Diagnosedetails

Element	Beschreibung
Kundenservice-Fall-ID	Gibt die Kundenservice-Fall-ID an, mit der die Supportanfrage eindeutig identifiziert wird. Der Symantec-Support ordnet Ihnen die entsprechende ID zu.
Details der Dateiübertragung	Zeigt die FTP-Übertragungsdetails an, die in der Supportanfrage konfiguriert sind. Die folgenden Informationen werden angezeigt: ■ "Symantec FTP-URL" - die FTP-Server-Adresse für den Symantec-Support. ■ "Benutzername" - das Benutzerkonto, das Sie für den Upload auf die Symantec-Support-FTP-Site verwenden. ■ "FTP-Verzeichnis" - der Pfad, in dem die hochgeladene Diagnoseergebnisdatei gespeichert wird. ■ Port - der Port, den die FTP-Site verwendet. Wenn die automatische Dateiübertragung in der Supportanfrage deaktiviert ist, wird dieses Element nicht angezeigt.
Ergebnisse der Diagnosedatensammlung	Zeigt die Ergebnisse der letzten Diagnosedatensammlung an. Die folgenden Informationen werden angezeigt: ■ "Ausgeführt am" - das Datum und die Uhrzeit, zu der die Diagnoseergebnisse gesammelt wurden. ■ "Status" - gibt an, ob die Diagnosedatensammlung erfolgreich war. Dieser Wert kann "Vollständig" oder "Vollständig mit Fehlern" sein. ■ "FTP-Status" - gibt an, ob die Diagnoseergebnisdatei erfolgreich zum Symantec-Support übertragen wurde. ■ "Fehler" - zeigt alle Fehler an, die während der Diagnosedatensammlung aufgetreten sind.

Sammeln von Protection Center-Diagnosedaten

Sie müssen Diagnosedaten aus Protection Center sammeln, wenn sie vom Symantec-Support dazu aufgefordert werden. Der Symantec-Support teilt Ihnen die Kundenservice-Fall-ID mit, die Sie für die Supportanfrage verwenden müssen. Außerdem gibt Ihnen der Symantec-Support die FTP-Übertragungsdetails, die Sie benötigen, um die Diagnoseergebnisdatei direkt aus Protection Center zu Symantec zu übertragen. Wenn eine benutzerdefinierte Konfigurationsdatei zum Sammeln der Diagnosedaten benötigt wird, stellt der Symantec-Support die entsprechende Datei ebenfalls zur Verfügung.

Siehe ["Hilfe vom Symantec-Support"](#) auf Seite 115.

Siehe ["Symantec-Support-Diagnoseoptionen"](#) auf Seite 116.

Sie müssen eine neue Supportanfrage erstellen und die folgenden Details angeben: Ihre Kundenservice-Fall-ID, die zu verwendende Konfigurationsdatei und die Daten für die Übertragung der Diagnosedatei. Wenn Sie die Details bestätigen, sammelt Protection Center die Diagnosedaten und zeigt eine Übersicht der Ergebnisse an.

Wenn Sie die entsprechenden FTP-Übertragungsdetails in der Supportanfrage angegeben haben, sendet Protection Center die Diagnoseergebnisdatei direkt an den Symantec-Support. Wenn Sie die Diagnoseergebnisdatei nicht direkt aus Protection Center übertragen, müssen Sie sie manuell an den Symantec-Support senden.

Hinweis: Protection Center unterstützt keine FTP-Proxy-Server. Wenn Ihre Umgebung einen Proxy-Server verwendet, müssen Sie die Diagnoseergebnisdatei speichern und manuell an den Symantec-Support senden.

So sammeln Sie Diagnosedaten für den Symantec-Support

- 1** Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Support-Diagnosen".
- 2** Klicken Sie auf der Support-Diagnoseseite auf "Neue Support-Anfrage erstellen".
- 3** Geben Sie im Dialogfeld "Neue Support-Anfrage starten" die entsprechenden Details an.

Siehe "[Supportanfrageneinstellungen](#)" auf Seite 120.

- 4

Klicken Sie auf "OK", um die Details zur Supportanfrage zu bestätigen.

Protection Center sammelt die Diagnosedaten und zeigt unter "Ergebnisse der Diagnosedatensammlung" eine Zusammenfassung an.

Wenn Sie die entsprechenden FTP-Übertragungsdetails in der Supportanfrage angegeben haben, sendet Protection Center die Diagnoseergebnisdatei direkt an den Symantec-Support.

Wenn die Diagnoseergebnisdatei nicht durch die Supportanfrage direkt zum Symantec-Support übertragen wird, können Sie die Diagnoseergebnisdatei später senden. Sie können die Datei direkt aus Protection Center übertragen oder Sie können die Datei herunterladen und manuell an den Symantec-Support senden.

Siehe ["Senden einer Diagnosedatei an den Symantec-Support"](#) auf Seite 123.

Siehe ["Speichern einer Diagnosedatei"](#) auf Seite 122.
- 5

(Optional) Wenn Sie die Supportanfrageneinstellungen ändern und die Diagnosedatensammlung wiederholen möchten, klicken Sie auf "Diagnose erneut ausführen".

Geben Sie im Dialogfeld "Support-Anfrage fortsetzen" die entsprechenden Details an.

Supportanfrageneinstellungen

Im Dialogfeld "Neue Support-Anfrage starten" können Sie eine neue Supportanfrage erstellen. Über das Dialogfeld "Support-Anfrage fortsetzen" können Sie die Diagnosedatensammlung erneut ausführen oder die aktuelle Diagnoseergebnisdatei an den Symantec-Support senden.

Siehe ["Hilfe vom Symantec-Support"](#) auf Seite 115.

Siehe ["Symantec-Support-Diagnoseoptionen"](#) auf Seite 116.

Siehe ["Sammeln von Protection Center-Diagnosedaten"](#) auf Seite 118.

Tabelle 11-5 Supportanfrageneinstellungen

Element	Beschreibung
Kundenservice-Informationen	Gibt die Kundenservice-Fall-ID an, mit der die Supportanfrage eindeutig identifiziert wird. Der Symantec-Support ordnet Ihnen die entsprechende ID zu, wenn Sie eine Supportanfrage stellen.

Element	Beschreibung
Konfigurationsdatei	Gibt an, welche Konfigurationsdatei zum Sammeln der Diagnosedaten aus Protection Center verwendet werden soll. Sie haben folgende Optionen: ■ Standardkonfigurationsdatei verwenden Die Standardkonfigurationsdatei befindet sich in Protection Center. Diese Konfigurationsdatei sammelt einen Standardsatz von Diagnosedaten aus Protection Center und ist für die Diagnose der meisten Probleme geeignet. ■ Benutzerdefinierte Konfigurationsdatei verwenden In einigen Fällen sammelt die Standardkonfigurationsdatei möglicherweise nicht die Daten, die der Symantec-Support benötigt, um das Problem zu diagnostizieren. Bei Bedarf stellt der Symantec-Support eine benutzerdefinierte Konfigurationsdatei bereit, die Sie dann verwenden müssen. Sie müssen die benutzerdefinierte Konfigurationsdatei an einem zugänglichen Speicherort ablegen und mithilfe dieser Option in Protection Center hochladen. Der Symantec-Support erstellt die benutzerdefinierten Konfigurationsdateien. Sie sind aus Sicherheitsgründen mit einer digitalen Signatur versehen und Sie können sie nicht ändern.

Element	Beschreibung
Diagnoseübertragungen	Gibt an, ob die Diagnoseergebnisse direkt aus Protection Center an den Symantec-Support gesendet werden oder ob sie gespeichert werden, damit Sie die Ergebnisdatei manuell senden können. Protection Center unterstützt keine FTP-Proxy-Server. Wenn Ihre Umgebung einen Proxy-Server verwendet, müssen Sie die Diagnoseergebnisdatei speichern und manuell an den Symantec-Support senden. Sie haben folgende Optionen: ■ Datei nicht mit Protection Center senden Die Diagnoseergebnisdatei wird in Protection Center gespeichert. Sie können die Datei später zum Symantec-Support übertragen oder Sie können die Datei herunterladen und manuell senden. ■ Datei mit Protection Center senden Die Diagnoseergebnisdatei wird am Ende des Sammlungsprozesses direkt zum Symantec-Support übertragen. Der Symantec-Support liefert die FTP-Übertragungsdetails, die Sie in den folgenden Feldern angeben müssen: ■ "URL des Symantec FTP-Servers" - die FTP-Server-Adresse für den Symantec-Support. ■ "FTP-Verzeichnis" - der Pfad, in dem die hochgeladene Diagnoseergebnisdatei gespeichert wird. ■ "Benutzername" - der Benutzername des Kontos, das Sie für den Upload auf die Symantec-Support-FTP-Site verwenden. ■ "Kennwort" - das Kennwort des Kontos, das Sie für den Upload auf die Symantec-Support-FTP-Site verwenden. ■ Port - der Port, den die FTP-Site verwendet. Der Standardport ist Port 21. FTP hat variable Ports, was möglicherweise Probleme verursacht, wenn Ihre Organisation Firewalls eingerichtet hat. Port 21 wird für die Steuerung verwendet, aber für die Datenübertragung kann jeder Port ab Port 1024 verwendet werden.

Speichern einer Diagnosedatei

Wenn Sie die Diagnosedatei nicht per FTP zu Symantec übertragen möchten, können Sie sie stattdessen per E-Mail senden. Beim Sammeln der Diagnosedaten wird die Diagnoseergebnisdatei in Protection Center gespeichert. Sie können die Diagnoseergebnisdatei aus Protection Center herunterladen, auf Ihrem lokalen Laufwerk speichern und anschließend manuell an den Symantec-Support senden.

Siehe ["Hilfe vom Symantec-Support"](#) auf Seite 115.

Siehe ["Symantec-Support-Diagnoseoptionen"](#) auf Seite 116.

Siehe ["Sammeln von Protection Center-Diagnosedaten"](#) auf Seite 118.

Siehe ["Supportanfrageneinstellungen"](#) auf Seite 120.

So speichern Sie eine Diagnosedatei

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Support-Diagnosen".
- 2 Klicken Sie auf der Symantec-Support-Diagnoseseite auf "Diagnosedatei speichern".
- 3 Klicken Sie im Dialogfeld "Datei-Download" auf "Speichern".
- 4 Geben Sie im Dialogfeld "Speichern unter" den entsprechenden Speicherort und den Dateinamen an und klicken Sie dann auf "Speichern".
- 5 Wenn der Download der Diagnoseergebnisdatei abgeschlossen ist, schließen Sie das Bestätigungsdialogfeld.

Senden einer Diagnosedatei an den Symantec-Support

In einigen Szenarien wird die Diagnoseergebnisdatei möglicherweise nicht beim Sammeln der Diagnosedaten zum Symantec-Support übertragen. Wenn Sie beispielsweise in der Supportanfrage keine FTP-Übertragungsdetails angeben oder wenn die Verbindung ausfällt, können die Ergebnisse nicht übertragen werden. Die Diagnoseergebnisdatei wird jedoch in Protection Center gespeichert und Sie können sie zum Symantec-Support übertragen, indem Sie die entsprechenden FTP-Übertragungsdetails angeben.

Siehe ["Hilfe vom Symantec-Support"](#) auf Seite 115.

Siehe ["Sammeln von Protection Center-Diagnosedaten"](#) auf Seite 118.

So senden Sie eine Diagnosedatei an den Symantec-Support

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Support-Diagnosen".
- 2 Klicken Sie auf der Symantec-Support-Diagnoseseite auf "Diagnosen an Support senden".

- 3 Geben Sie im Dialogfeld "Support-Anfrage fortsetzen" unter "Diagnosedatei-Übertragungseinstellungen" die entsprechenden FTP-Übertragungseinstellungen an.

Siehe ["Supportanfrageneinstellungen"](#) auf Seite 120.

- 4 Klicken Sie auf "OK".

Die Diagnoseergebnisse werden aus Protection Center zum Symantec-Support übertragen. Die Details unter "Ergebnisse der Diagnosedatensammlung" werden entsprechend aktualisiert.

Siehe ["Symantec-Support-Diagnoseoptionen"](#) auf Seite 116.

Sicherheitsmanagement

- [Kapitel 12. Einleitung zum Sicherheitsmanagement mit Protection Center](#)
- [Kapitel 13. Verwenden von Protection Center-Berichten](#)
- [Kapitel 14. Arbeiten mit Benachrichtigungen](#)
- [Kapitel 15. Arbeiten mit Arbeitsabläufen und Aufgaben](#)

Einleitung zum Sicherheitsmanagement mit Protection Center

In diesem Kapitel werden folgende Themen behandelt:

- [Ausführung von Sicherheitsmanagement-Aufgaben in Protection Center](#)
- [Info zum Protection Center-Dashboard](#)
- [Zugriff auf die Verwaltungsschnittstelle eines unterstützten Produkts](#)

Ausführung von Sicherheitsmanagement-Aufgaben in Protection Center

Die Rolle eines Sicherheitsmanagers besteht darin, sicherzustellen, dass das Netzwerk der Organisation sicher ist. Ihre Organisation hat möglicherweise einen einzelnen Sicherheitsmanager mit voller Verantwortung für die Netzwerksicherheit. Alternativ kann Ihre Organisation mehrere Sicherheitsmanager haben, die jeweils für einen anderen Aspekt Ihrer Sicherheit verantwortlich sind.

Wenn Sie Sicherheitsmanager sind, sollten Sie sich mit Sicherheitsmanagement-Aufgaben vertraut machen, bevor Sie Protection Center erstmals verwenden. Sie brauchen keine Erstkonfiguration von Protection Center durchzuführen, bevor Sie anfangen, mithilfe von Protection Center Sicherheitsmanagement-Aufgaben auszuführen. Sie sollten jedoch die Berichte konfigurieren, die Sie regelmäßig verwenden möchten, und sie als gespeicherte Berichte ablegen.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Die folgende Tabelle beschreibt den Prozess zum Ausführen von Sicherheitsmanagement-Aufgaben in Protection Center.

Tabelle 12-1 Prozess zum Ausführen von Sicherheitsmanagement-Aufgaben in Protection Center

Schritt	Aufgabe	Beschreibung
Schritt 1	Loggen Sie sich bei Protection Center ein.	Wenn Sie bei sich Protection Center einloggen, befinden Sie sich in der Ansicht "Protection Center". Diese Ansicht bietet Zugriff auf alle Protection Center-Funktionen. Siehe "Zugriff auf Protection Center" auf Seite 18.
Schritt 2	Zeigen Sie das Dashboard an.	Auf dem Dashboard erhalten Sie schnell einen Überblick über den aktuellen Status Ihrer Sicherheit. Siehe "Info zum Protection Center-Dashboard" auf Seite 129.
Schritt 3	Verwenden Sie Berichte.	Berichte basieren auf Daten aus den unterstützten Produkten und helfen Ihnen, den Status Ihrer Netzwerk- und Endgeräteumgebung festzustellen. Siehe "Info zu Berichten" auf Seite 133.
Schritt 4	Verwenden Sie Geschäftsanalysen.	Die Geschäftsanalysefunktion in Protection Center bietet mehrdimensionale Analysen und zuverlässige grafische Berichterstellung, die Sie bei der Analyse Ihrer Daten unterstützen. Siehe "Info zu Geschäftsanalysen in Protection Center" auf Seite 27.
Schritt 5	Verwenden Sie Workflows.	Protection Center stellt Workflows bereit, um Ihr Sicherheitsmanagement zu vereinfachen und Ihnen zu helfen, eine sichere Umgebung zu erhalten. Wenn Sie eine Aktion in einem Bericht auswählen, startet Protection Center den entsprechenden Workflow auf dem entsprechenden Endgerät. Siehe "Info zu Workflows" auf Seite 151.
Schritt 6	Arbeiten Sie mit Benachrichtigungen.	Benachrichtigungen sind die Meldungen, die Sie laufend über bedeutende Ereignisse in Protection Center und in integrierten Produkten informieren. Protection Center generiert Benachrichtigungen für alle wichtigen Ereignisse oder Aktivitäten, die in Protection Center auftreten oder in einem integrierten Produkt erkannt werden. Siehe "Info zu Benachrichtigungen" auf Seite 147.
Schritt 7	Verwalten Sie Produkte.	Protection Center ermöglicht das Verwalten Ihrer Sicherheitsprodukte über die Protection Center-Schnittstelle. Siehe "Zugriff auf die Verwaltungsschnittstelle eines unterstützten Produkts" auf Seite 131.

Info zum Protection Center-Dashboard

Das Protection Center-Dashboard wird immer als Erstes angezeigt, wenn Sie sich bei Protection Center einloggen. Hier können Sie den aktuellen Status Ihrer Sicherheit anzeigen und Sicherheitsereignisse entsprechend Ihrer Benutzerrolle und Ihren Administratorberechtigungen verwalten.

Siehe ["Erste Schritte mit Protection Center"](#) auf Seite 17.

Siehe ["Ausführung von Sicherheitsmanagement-Aufgaben in Protection Center"](#) auf Seite 127.

Das Protection Center-Dashboard enthält einige Diagramme und einen Newsfeed. Der Newsfeed zeigt die wichtigsten oder neuesten Benachrichtigungen an. Die Diagramme zeigen die zusammenfassenden Informationen an, die Ihnen einen Überblick über den aktuellen Status Ihrer Sicherheit geben. In einigen Diagramme können Sie einen Drilldown zu den Zusammenfassungsdaten durchführen, um zusätzliche Einzelheiten anzuzeigen.

Tabelle 12-2 Im Protection Center-Dashboard bereitgestellte Informationen

Diagramm	Beschreibung
Produktionsüberblick	Stellt eine Übersicht über Malware, Sicherheitslücken und Spamdaten zur Verfügung. Die Übersichtsinformationen umfassen für jeden Typ Daten Folgendes: ein Liniendiagramm der Aktivität in den vorherigen 24 Stunden, einen Zählwert und die prozentuale Veränderung seit dem vorherigen 24-Stunden-Zeitraum. Jede Datenzeile verfügt über einen Link zu den entsprechenden zusammenfassenden Berichten auf höchster Ebene, wie zum Beispiel "Malware-Zusammenfassung" und "E-Mail".

Diagramm	Beschreibung
Produktserversstatus	Zeigt den gesamten Konnektivitätsstatus für alle Produktservers an. Der Status spiegelt den Zustand der Datenfluss-Verbindungen wider. Die Werte für den Hoststatus lauten wie folgt: ■ Gut Die Gesamtzahl von Produktserversn, die eine Verbindung hergestellt und keine Agent- oder Datenflussprobleme haben. Ein angehaltenes Produkt auf einem verbundenen Server ist ein Datenflussproblem. ■ Warnung Ein Server hat einen veralteten Symantec Management-Agent oder ein veraltetes Plugin oder es gibt ein Datenflussproblem. Das Produkt ist angehalten oder es gibt ein Problem mit der Benutzer-ID, die für den Datenflusszugriff verwendet wird. ■ Fehler Die Kommunikation mit einem vorher integrierten Produkt ist fehlgeschlagen. ■ Nicht aktiviert Ein Produktservers ist für die Integration verfügbar, wurde aber noch nicht aktiviert.
Produktintegrationsstatus	Zeigt Informationen über die Sicherheitsabdeckung an, die Protection Center in Ihrer Umgebung erzielt. Daraus können Sie entnehmen, wie viele unterstützten Produkte Sie derzeit integriert haben und wie viele weitere verfügbar sind, aber nicht aktiviert wurden.
Systemstatus	Zeigt den Status der kritischen Komponenten der Protection Center-Appliance an. Dieses Fenster liefert Informationen zu Protection Center-Systemverfügbarkeit, CPU-Auslastung, Speicherauslastung und Datenträgerbelegung.
Newsfeed	Zeigt eine Liste aller Benachrichtigungen an, die in Protection Center nachverfolgt werden. Benachrichtigungen können Warnungen, Ereignisse oder Informationsmeldungen sein. Benachrichtigungen können sich auf Sicherheitsprodukte beziehen, auf die Protection Center-Infrastruktur oder auf das Global Intelligence Network. Sie können die Liste nach Priorität oder nach Datum sortieren. Jedes Benachrichtigungselement im Newsfeed umfasst ein Schweregradsymbol, einen Zeitstempel, einen Namen und eine ausführliche Beschreibung. Der Link "Vollständige Liste anzeigen" öffnet den Bericht "Benachrichtigungen". Siehe "Benachrichtigungsdetails" auf Seite 149.
Threatcon-Status	Zeigt den aktuellen Threatcon-Status an und ermöglicht den Zugriff auf Definitionen von Sicherheitsbenachrichtigungen. Symantec Endpoint Protection liefert diese Informationen.
DeepSight-Anzeige	Zeigt die DeepSight-Informationen an, auf die Sie Zugriff haben. DeepSight ist ein Symantec-Dienst, der Sicherheitsereignisse global überwacht und Frühwarn-Benachrichtigungen über Angriffe liefert.

Diagramm	Beschreibung
Die wichtigsten Bedrohungen für Unternehmen	Zeigt eine Liste der wichtigsten Bedrohungen durch bösartige Software an, denen Organisationen derzeit gegenüberstehen.

Zugriff auf die Verwaltungsschnittstelle eines unterstützten Produkts

Sie können über das Produktauswählménú in Protection Center auf die Verwaltungsschnittstelle eines unterstützten Produkts zugreifen. Das Produktauswählménú befindet sich links neben dem Ménú "Startseite" und zeigt den Namen des momentan ausgewählten Produkts an. Wenn Sie auf das Produktauswählménú klicken, wird eine Dropdown-Liste mit aktivierten Produkten angezeigt. Das vordefinierte Protection Center-Administratorkonto (SPC_Admin) hat uneingeschränkten Zugriff auf unterstützte Produkte. Den Protection Center-Benutzerkonten müssen die entsprechenden Berechtigungen für den Zugriff auf unterstützte Produkte zugewiesen werden.

Siehe ["Info zu unterstützten Produkten"](#) auf Seite 29.

Siehe ["Integrieren unterstützter Produkte"](#) auf Seite 30.

Siehe ["Über Protection Center-Benutzerkonten"](#) auf Seite 56.

Siehe ["Unterstützte Produktzugriffsberechtigungseinstellungen"](#) auf Seite 75.

So greifen Sie auf die Verwaltungsschnittstelle eines unterstützten Produkts zu

- 1 Klicken Sie in Protection Center in der Produktauswahl auf den nach unten zeigenden Pfeil.
- 2 Klicken Sie auf "Produktname > Hostname".
Die Startseite der Produktverwaltungsschnittstelle öffnet sich.
- 3 Führen Sie die entsprechenden Verwaltungsfunktionen aus.
Informationen zur Anwendung der Produktfunktionen finden Sie in der Hilfedokumentation für dieses Produkt. Klicken Sie dazu im Navigationsbereich auf "Hilfe".

Verwenden von Protection Center-Berichten

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Berichten](#)
- [Info zu Diagrammen](#)
- [Info zu Berichtsaktionen](#)
- [Info zu Berichtsfiltern](#)
- [Anzeigen eines Berichts](#)
- [Anwenden von Filtern auf einen Bericht](#)
- [Erstellen gespeicherter Berichte](#)
- [Löschen eines gespeicherten Berichts](#)
- [Konfigurieren der Verteilung eines Berichts](#)
- [Berichtsverwaltungseinstellungen](#)
- [Berichtsverteilungseinstellungen](#)
- [Info zu speziellen Berichten für Mail Security](#)

Info zu Berichten

Protection Center liefert Berichte, die Ihre Organisation jederzeit über Sicherheitsprobleme informieren und die Ihnen die schnelle Reaktion auf Sicherheitsereignisse erleichtern. Die Daten in den Berichten werden durch die integrierten Produkte in Ihrer Umgebung sowie durch Protection Center geliefert.

Welche Berichtsdaten Sie anzeigen können, ist von den Berechtigungen des Kontos abhängig, dem Ihr Protection-Benutzerkonto zugeordnet ist.

Siehe "[Anzeigen eines Berichts](#)" auf Seite 136.

Berichtsdaten werden in Diagrammen organisiert, damit die Daten einfach zu lesen und zu analysieren sind. Beispielsweise ermöglicht ein Kreisdiagramm die mühelose Identifizierung der verschiedenen Kategorien blockierter Malware. Anhand dieser Informationen können Sie schnell erkennen, ob bei Ihnen mögliche Sicherheitslücken vorhanden sind. Bei einigen Diagrammen können Sie auch Aktionen als Reaktion auf gemeldete Ereignisse durchführen.

Bei jedem Bericht können Sie auch Filter anwenden, damit Sie nur die Informationen sehen, die Sie als für Ihre Situation relevant betrachten. Wenn Sie vorhaben, später erneut auf denselben Satz gefilterter Daten zuzugreifen, können Sie den Bericht und seine Filter unter einem neuen Namen speichern. Sie können dann, wenn Sie diesen speziellen Satz von Daten wieder benötigen, den gespeicherten Bericht öffnen.

Siehe "[Info zu Diagrammen](#)" auf Seite 134.

Siehe "[Info zu Berichtsaktionen](#)" auf Seite 135.

Siehe "[Info zu Berichtsfiltern](#)" auf Seite 135.

Siehe "[Erstellen gespeicherter Berichte](#)" auf Seite 139.

Um sicherzustellen, dass Mitarbeiter genau die Sicherheitsinformationen erhalten, die sie benötigen, können Sie planen, wann ein Bericht an wen verteilt werden soll. Die Berichtsempfänger können den Bericht dann anzeigen, ohne sich bei Protection Center einzuloggen.

Siehe "[Konfigurieren der Verteilung eines Berichts](#)" auf Seite 141.

Bei Produkten, die mit Protection Center integriert sind, sind möglicherweise auch eigene produktspezifische Berichte vorhanden. Wenn Sie z. B. Mail Security mit Protection Center integriert haben, werden spezielle Berichte für Mail Security verfügbar.

Siehe "[Info zu speziellen Berichten für Mail Security](#)" auf Seite 144.

Info zu Diagrammen

Ein Diagramm ist eine Komponente eines Berichts, in der Daten mithilfe einer einheitlichen Methode in strukturierter und leicht zu analysierender Form angezeigt werden. Die gängigsten Formen von Diagrammen sind Kreisdiagramm, Balkendiagramm, Bereichsdiagramm, Liniendiagramm und Tabelle.

Siehe "[Info zu Berichten](#)" auf Seite 133.

Jeder Bericht umfasst ein oder mehrere Diagramme. Bei einigen Diagrammen können Sie Drilldowns durchführen, um ausführlichere Informationen über die Daten zu erhalten. Manche Diagrammen lassen die Ausführung bestimmter Aktionen für die Diagrammdaten zu. Diese Aktionen vereinfachen die Problemlösung.

Siehe ["Info zu Berichtsaktionen"](#) auf Seite 135.

Info zu Berichtsaktionen

Mithilfe von Berichtsaktionen können Sie die Aufgaben durchführen, die erforderlich sind, um die Sicherheit Ihrer Endgeräte sicherzustellen. Beispielsweise können Sie mithilfe einer Aktion einen Computer isolieren, auf dem nicht die neuesten Virendefinitionen installiert sind.

Siehe ["Info zu Berichten"](#) auf Seite 133.

Mit Diagrammen, die ausführliche Informationen enthalten, z. B. den Diagrammen in Detailberichten, sind häufig Aktionen verbunden. Welche Aktionen verfügbar sind, ist von den Daten im Diagramm und den von Protection Center unterstützten Produkten abhängig, die bei Ihnen verfügbar sind.

Siehe ["Info zu Diagrammen"](#) auf Seite 134.

Wenn Aktionen für einen Bericht verfügbar sind, wird das Menü "Aktionen" am oberen Ende des betreffenden Diagramms angezeigt. Um eine Aktion auf einem Endgerät durchzuführen, wählen Sie das entsprechende Element im Diagramm aus und wählen Sie dann die gewünschte Aktion im Menü.

Siehe ["Info zu Workflows"](#) auf Seite 151.

Die Optionen im Menü "Aktionen" sind mit Workflows verknüpft. Wenn Sie eine Menüoption wählen, starten Sie den entsprechenden Workflow.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

Info zu Berichtsfiltern

Sie können Filter auf einen Bericht anwenden, damit dieser nur die Daten anzeigt, die Sie sehen möchten.

Siehe ["Info zu Berichten"](#) auf Seite 133.

Die Option "Filter hinzufügen" ermöglicht den Zugriff auf die Filter, die in einem Bericht verfügbar sind. Die Verwendung von Berichtsfiltern ist optional; Sie können einige oder alle verfügbaren Filter verwenden.

Sie können die folgenden Richtlinien verwenden, wenn Sie Filter auf einen Bericht anwenden:

- Jeder Filter entspricht einer Datenspalte im Bericht.
- Für jeden Filter können Sie einen Parameterwert angeben.
- Sie können mehrere Filter für dieselbe Datenspalte hinzufügen.
- Bei jedem Filter wird der Parameterwert dem Datenwert zugeordnet, wobei entweder durchsuchter Werte oder uneingeschränkter Text verwendet wird.

Berichtsfilter unterstützen Suchvorgänge nach Wortteilen, sie unterstützen jedoch keine Platzhalterzeichen. Die Platzhalterzeichen "?" und "*" werden nicht als Platzhalter, sondern als normale Zeichen interpretiert.

Die Filter, die Sie einem Bericht hinzugefügt haben, werden im Berichtsheader auf der linken Seite gezeigt. Auf der rechten Seite des Berichtsheaders können Sie auf die vordefinierten Filter für Zeiträume zugreifen. Mithilfe dieser Filter können Sie die Daten anzeigen, die am Vortag, in der vorherigen Woche, im vorherigen Monat oder in den vorherigen drei Monaten gesammelt wurden. Hier können Sie auch das Startdatum und das Enddatum eines benutzerdefinierten Zeitraums angeben.

Siehe ["Anzeigen eines Berichts"](#) auf Seite 136.

Die Filter, die Sie auf einen Bericht anwenden, werden gelöscht, wenn Sie von dem Bericht weg navigieren. Wenn Sie eine bestimmte Filterkonfiguration für einen Standardbericht beibehalten möchten, können Sie unter Verwendung der Option "Speichern unter" einen gespeicherten Bericht erstellen. Wenn Sie das nächste Mal auf den gespeicherten Bericht zugreifen, werden die von Ihnen festgelegten Filter automatisch angewendet. Darüber hinaus können Sie die neuen und geänderten Filtereinstellungen unter Verwendung der Option "Speichern" oben auf der Berichtsseite in einem gespeicherten Bericht speichern.

Siehe ["Erstellen gespeicherter Berichte"](#) auf Seite 139.

Anzeigen eines Berichts

Sie können einen Protection Center-Bericht anzeigen. Es ist möglich, die Ergebnisse eines Berichts weiter zu präzisieren, indem Sie mithilfe von Filtern einige Daten ausblenden und nur die Berichtsergebnisse beibehalten, die Sie anzeigen möchten. Die Daten können nach einer bestimmten Spalte sortiert werden. Wenn Sie einen Bericht aktualisieren, werden die Filter und die Einstellungen zum Sortieren der Daten beibehalten.

Siehe ["Info zu Berichten"](#) auf Seite 133.

Siehe ["Info zu Berichtsfiltern"](#) auf Seite 135.

Wenn keine Daten im Bericht verfügbar sind, zeigt Protection Center eine entsprechende Meldung an. Möglicherweise sind keine Daten verfügbar, weil keine integrierten Produkte vorhanden sind, die die entsprechenden Daten liefern könnten. Es ist auch möglich, dass die Produkte integriert sind, Ihr Benutzerkonto jedoch keinem Produktkonto zugeordnet ist, das über Berechtigungen für diese Produktdaten verfügt. Protection Center zeigt außerdem eine Liste der unterstützten Produkte an, die den Bericht aktivieren können.

So zeigen Sie einen Bericht an

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 Im linken Teilfenster wählen Sie die entsprechende Liste von Berichten aus:

Standardberichte anzeigen

Klicken Sie auf das Symbol "Berichte".

Gespeicherte Berichte anzeigen

Klicken Sie auf das Symbol "Gespeicherte Berichte".

- 3 In der Liste der Berichte klicken Sie auf den Bericht, den Sie anzeigen möchten.
- 4 (Optional) Geben Sie im Dialogfeld "Geben Sie die folgenden erforderlichen Parameter ein" den entsprechenden Wert an und klicken Sie dann auf "Filter übernehmen".

Wenn Sie Parameter für den Bericht angeben müssen, fordert Protection Center Sie zur Eingabe der benötigten Informationen auf.

Wenn der Parameter durchsuchte Werte verwendet, können Sie den benötigten Wert in einer Dropdown-Liste wählen. Wenn der Parameter einen beliebigen Wert annehmen kann, müssen Sie eine passende Zeichenkette eingeben. Die Berichtsergebnisse umfassen alle Zeichenketten, die ganz oder teilweise mit der angegebenen Filterzeichenkette übereinstimmen.

Standardmäßig umfasst jeder Bericht die Daten, die Protection Center während der letzten sieben Tage gesammelt hat.

- 5 (Optional) Geben Sie im Berichtsheader den Zeitraum für die Daten an, die Sie anzeigen möchten.

Sie können einen der vordefinierten Zeiträume wählen oder einen benutzerdefinierten Zeitraum festlegen.

- 6 (Optional) Konfigurieren Sie im Berichtsheader alle Filter, die Sie auf den Bericht anwenden möchten.

Siehe ["Anwenden von Filtern auf einen Bericht"](#) auf Seite 138.

- 7 (Optional) Klicken Sie auf ein Diagramm, um einen Drilldown zu einem ausführlicheren Bericht durchzuführen.

Die Filterparameter, die dem Element entsprechen, auf das Sie geklickt haben, werden auf den ausführlichen Bericht angewendet.

Anwenden von Filtern auf einen Bericht

Sie können Filter auf einen Bericht anwenden, um die Ergebnisse zu präzisieren und nur die gewünschten Berichtsergebnisse anzuzeigen. Jeder Filter entspricht einer der Datenspalten im Bericht. Für jeden Filter kann nur ein Parameterwert festgelegt werden. In manchen Fällen können Sie jedoch mehrere Filter desselben Typs mit jeweils verschiedenen Parameterwerten hinzufügen. Der Parameterwert in jedem Filter wird mit den Datenwerten in der entsprechenden Spalte im Bericht abgeglichen und alle übereinstimmenden Ergebnisse werden angezeigt.

Siehe ["Anzeigen eines Berichts"](#) auf Seite 136.

Wenn die Datenspalte, die Sie filtern möchten, durchsuchte Werte enthält, können Sie unter den verfügbaren Werten den gewünschten wählen. Wenn die Datenspalte uneingeschränkten Text enthält, können Sie eine benutzerdefinierte Textzeichenkette angeben.

Siehe ["Info zu Berichtsfiltern"](#) auf Seite 135.

Die Filter, die Sie einem Bericht hinzugefügt haben, werden im Berichtsheader auf der linken Seite gezeigt. Sie können Filter ändern, indem Sie verschiedene Parameterwerte angeben, und Sie können alle Filter entfernen, die Sie nicht mehr benötigen. Die erforderlichen Filter in ausführlichen Berichten können jedoch nicht entfernt werden.

So fügen Sie einem Bericht einen Filter hinzu

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 In der Liste der Berichte klicken Sie auf den Bericht, den Sie anzeigen möchten.

- 3 Im Berichtsheaderbereich klicken Sie auf "Filter hinzufügen".
- 4 In der Dropdown-Liste wählen Sie den entsprechenden Filterparameter. Anschließend haben Sie folgende Möglichkeiten:

Durchsuchten Wert wählen	Klicken Sie auf den Wert, den Sie verwenden möchten.
Benutzerdefinierten Wert angeben	Klicken Sie auf "Benutzerdefinierter Filter", geben Sie den entsprechenden Wert ein und klicken Sie auf "Filter übernehmen".

Beachten Sie, dass bei manchen Filter das Erstellen benutzerdefinierter Filter nicht möglich ist.

So bearbeiten Sie einen Filter

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 In der Liste der Berichte klicken Sie auf den Bericht, den Sie anzeigen möchten.
- 3 Im Berichtsheader klicken Sie auf den Filter, den Sie bearbeiten möchten.
- 4 In der Dropdown-Liste wählen Sie eine der folgenden Optionen:
 - Klicken Sie auf den Wert, den Sie verwenden möchten.
 - Klicken Sie auf "Benutzerdefinierter Filter", geben Sie den entsprechenden Wert ein und klicken Sie auf "Filter übernehmen".

Beachten Sie, dass bei manchen Filter das Erstellen benutzerdefinierter Filter nicht möglich ist.

So entfernen Sie einen Filter

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 In der Liste der Berichte klicken Sie auf den Bericht, den Sie anzeigen möchten.
- 3 Klicken Sie im Berichtsheader in dem Filter, den Sie entfernen möchten, auf das Symbol "Löschen" (X).

Erforderliche Filter können nicht aus Berichten entfernt werden. Für erforderliche Filter steht das Symbol "Löschen" nicht zur Verfügung.

Erstellen gespeicherter Berichte

Sie können einen gespeicherten Bericht erstellen, indem Sie einen Bericht unter einem neuen Namen speichern.

Siehe ["Info zu Berichten"](#) auf Seite 133.

So können Sie z. B. Filter auf einen Bericht anwenden oder seine Verteilung konfigurieren und anschließend eine Kopie des Berichts unter einem neuen Namen speichern. Wenn Sie auf den gespeicherten Bericht zugreifen, sind seine Filter und Verteilungseinstellungen bereits vorhanden; Sie brauchen sie nicht erneut anzugeben. Stattdessen können Sie den gespeicherten Bericht schnell anzeigen und anhand der Berichtsdaten die nötigen Aktionen durchführen.

Siehe ["Konfigurieren der Verteilung eines Berichts"](#) auf Seite 141.

Siehe ["Anzeigen eines Berichts"](#) auf Seite 136.

Siehe ["Info zu Berichtsaktionen"](#) auf Seite 135.

Sie können einen gespeicherten Bericht verwenden, um zusätzliche benutzerdefinierte Berichte zu erstellen. Beispielsweise können Sie einen gespeicherten Bericht ändern und ihn dann unter einem anderen Namen speichern.

Sie können einen gespeicherten Bericht auch löschen.

Siehe ["Löschen eines gespeicherten Berichts"](#) auf Seite 141.

Die gespeicherten Berichte, die Sie erstellen, sind für alle Protection Center-Benutzer verfügbar.

So erstellen Sie einen gespeicherten Bericht

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 Im linken Teilfenster wählen Sie die entsprechende Liste von Berichten aus:

Standardberichte anzeigen

Klicken Sie auf das Symbol "Berichte".

Gespeicherte Berichte anzeigen

Klicken Sie auf das Symbol "Gespeicherte Berichte".

- 3 In der Liste der Berichte klicken Sie auf den Bericht, den Sie anzeigen möchten.
- 4 Konfigurieren Sie im Berichtsheader die Filter, die Sie auf den Bericht anwenden möchten.

Siehe ["Anwenden von Filtern auf einen Bericht"](#) auf Seite 138.

- 5 Klicken Sie oben auf der Berichtsseite auf "Speichern unter".
- 6 Geben Sie im Dialogfeld "Kopie von <Berichtsname> speichern unter" im Feld "Berichtsname" den Namen des neuen gespeicherten Berichts ein und klicken Sie dann auf "Speichern".

Löschen eines gespeicherten Berichts

Sie können einen gespeicherten Bericht löschen, wenn Sie ihn nicht mehr benötigen. Die Standardberichte von Protection Center können nicht gelöscht werden.löschen

Siehe ["Info zu Berichten"](#) auf Seite 133.

So löschen Sie einen gespeicherten Bericht

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 Im linken Teilfenster klicken Sie auf das Symbol "Gespeicherte Berichte".
- 3 In der Liste der Berichte klicken Sie auf den Bericht, den Sie löschen möchten.
- 4 Klicken Sie oben im Bericht auf "Löschen".

Konfigurieren der Verteilung eines Berichts

Bei den meisten Berichten in Protection Center können Sie einen Zeitplan für die regelmäßige Erstellung konfigurieren. Außerdem können Sie die Verteilung der Ergebnisse an die gewünschten Empfänger per E-Mail konfigurieren. Protection Center generiert den Bericht zu den geplanten Terminen und bezieht dabei die Daten ein, die zum jeweiligen Zeitpunkt verfügbar sind. Welche Daten in den Bericht aufgenommen werden, ist von den Produktzugriffsberechtigungen des Benutzers abhängig, der den Bericht zuletzt gespeichert hat. Protection Center sendet den Bericht als HTML-Dateianhang oder als Link zum Bericht an die E-Mail-Adressen auf der angegebenen Liste.

Siehe ["Info zu Berichten"](#) auf Seite 133.

Einige Berichte benötigen einen oder mehrere Parameter, bevor sie ausgeführt werden können. Um die Verteilung für einen solchen Bericht zu planen, müssen Sie eine Kopie des Berichts speichern, in der die entsprechenden Parameter festgelegt sind. Anschließend können Sie die Verteilung des gespeicherten Berichts planen.

Siehe ["Erstellen gespeicherter Berichte"](#) auf Seite 139.

Es ist auch möglich, den Namen und die Beschreibung eines gespeicherten Berichts zu ändern. Die Namen und Beschreibungen der Standardberichte von Protection Center können nicht geändert werden.

So konfigurieren Sie die Verteilung eines Berichts

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 Im linken Teilfenster klicken Sie auf "Berichte verwalten".

- 3

Wählen Sie im Dialogfeld "Berichte verwalten" im linken Teilfenster die Liste von Berichten aus, die Sie anzeigen möchten:

So zeigen Sie die Liste von Standardberichten an

Klicken Sie auf "Protection Center".

So zeigen Sie die Liste gespeicherter Berichte an

Klicken Sie auf "Gespeichert".
- 4

Klicken Sie im oberen Teil des rechten Teilfensters auf den Bericht, den Sie ändern möchten.
- 5

(Optional) Nehmen Sie im unteren Teil des rechten Teilfensters die gewünschten Änderungen am Berichtsnamen und an der Beschreibung vor.

Siehe "Berichtsverwaltungseinstellungen" auf Seite 142.
- 6

Führen Sie im Feld "Drilldowns" einen der folgenden Schritte aus:

Wenn kein Zeitplan konfiguriert ist

Klicken Sie auf "Zeitplan und Empfänger angeben".

Wenn bereits ein Zeitplan bereits konfiguriert ist

Klicken Sie auf "Bearbeiten".
- 7

Im Dialogfeld "Zeitplan bearbeiten" geben Sie die entsprechenden Berichtsverteilungsoptionen an.

Siehe "Berichtsverteilungseinstellungen" auf Seite 143.
- 8

Klicken Sie auf "Speichern".
- 9

Klicken Sie auf "Schließen".

Berichtsverwaltungseinstellungen

Mithilfe der Berichtsverwaltungseinstellungen können Sie Protection Center-Berichte anzeigen und ändern.

Siehe "[Konfigurieren der Verteilung eines Berichts](#)" auf Seite 141.

Tabelle 13-1 Berichtsverwaltungseinstellungen

Element	Beschreibung
Name	Enthält den Berichtsnamen. Der Name eines Standardberichts in Protection Center kann nicht geändert werden.

Element	Beschreibung
Beschreibung	Enthält die Beschreibung des Berichts. Die Beschreibung eines Standardberichts in Protection Center kann nicht geändert werden.
Besitzer	Gibt das Protection Center-Benutzerkonto an, das den Bericht gespeichert hat. Diese Einstellung ist nur bei gespeicherten Berichten vorhanden. Sie ist lediglich ein informativer Hinweis und kann nicht geändert werden.
Verteilung	Gibt den Zeitplan für die Erstellung des Berichts und der E-Mail-Adressen der Empfänger an. Protection Center generiert den Bericht zu den geplanten Terminen und bezieht dabei die Daten ein, die zum jeweiligen Zeitpunkt verfügbar sind. Welche Daten in den Bericht aufgenommen werden, ist von den Produktzugriffsberechtigungen des Benutzers abhängig, der den Bericht zuletzt gespeichert hat. Protection Center sendet den Bericht als HTML-Dateianhang oder als Link zum Bericht an die E-Mail-Adressen auf der angegebenen Liste.
Bericht öffnen	Öffnet den Bericht in Protection Center.

Berichtsverteilungseinstellungen

Die Berichtsverteilungseinstellungen ermöglichen es, die Erstellung beliebiger Protection Center-Berichte und ihrer E-Mail-Verteilung zu planen.

Siehe "[Konfigurieren der Verteilung eines Berichts](#)" auf Seite 141.

Tabelle 13-2 Verteilungszeitplaneinstellungen

Element	Beschreibung
Keine	Deaktiviert die geplante Verteilung für den Bericht.
Täglich	Verteilt Berichte jeden Tag oder in den angegebenen Zeitabständen (von mehreren Tagen) zur angegebenen Uhrzeit.
Wöchentlich	Verteilt Berichte jede Woche zur angegebenen Uhrzeit am angegebenen Wochentag.
Monatlich	Verteilt Berichte jeden Monat am angegebenen Datum und zur angegebenen Zeit. Bei allen Einstellungen zur Verteilungshäufigkeit können Sie ein Start- und ein Enddatum festlegen.

Tabelle 13-3 Empfänger und E-Mail-Einstellungen

Element	Beschreibung
Empfänger	Gibt die E-Mail-Adressen an, an die Protection Center die Berichtsergebnisse sendet. Eine E-Mail wird jedes Mal gesendet, wenn Protection Center den Bericht entsprechend dem angegebenen Zeitplan generiert. Wenn Sie mehrere E-Mail-Adressen angeben, müssen Sie die einzelnen Adressen durch Komma oder Semikolon trennen.
E-Mail-Format	Gibt an, ob die Berichtsergebnisse direkt im HTML-Format oder als Link zum eigentlichen Bericht gesendet werden sollen. Beachten Sie, dass einige Berichte das HTML-Format nicht unterstützen. Beispielsweise können die Ergebnisse des Berichts "Benachrichtigungen" nur als Link per E-Mail verschickt werden. Wenn die Berichtsergebnisse als angehängtes HTML-Dokument verschickt werden, werden der Ergebnisbereich entsprechend dem Benutzer festgelegt, der den Bericht zuletzt gespeichert hat. Wenn die E-Mail einen Link zu dem Bericht enthält, muss jeder Empfänger sich bei Protection Center einloggen, um die Berichtsergebnisse zu sehen. Der Ergebnisbereich wird entsprechend dem Benutzerkonto festgelegt, das zum Einloggen bei Protection Center verwendet wird.
E-Mail-Betreff	Gibt die Betreffzeile der E-Mail an, die die Berichtsergebnisse enthält.
E-Mail	Gibt die E-Mail-Nachricht an, die zusammen mit dem Bericht gesendet wird.

Info zu speziellen Berichten für Mail Security

Wenn Sie Mail Security in Protection Center aktivieren, werden einige für Mail Security spezifische Berichte der Liste der in Protection Center verfügbaren Berichte hinzugefügt. Mithilfe dieser Berichte können Sie die Daten anzeigen, die Protection Center von den integrierten Mail Security-Servern gesammelt hat. Die Daten, die in einigen Standardberichten von Protection Center angezeigt werden, sind Mail Security-Daten sowie Daten, die von anderen integrierten Produkten gesammelt wurden.

Siehe ["Integrieren von Mail Security in Protection Center"](#) auf Seite 42.

Tabelle 13-4 Spezielle Berichte für Mail Security in Protection Center

Berichtsname	Beschreibung
SMSMSE – Inhaltsfilterungsbericht	Zeigt zusammenfassende Informationen zu E-Mail-Inhalten in Ihrer Organisation an. Dieser Bericht enthält die folgenden Diagramme: ■ Filterungsverletzungen wichtiger Inhalte ■ Abgefangene Inhalte - Trend ■ Erste Anlagen ■ Erste Absender (eingehend/ausgehend)
SMSMSE - Umgebungszusammenfassung	Zeigt zusammenfassende Informationen zur E-Mail-Umgebung in Ihrer Organisation an. Dieser Bericht enthält die folgenden Diagramme: ■ MSMSE-Dienststatus ■ Virusdefinitionsstatus ■ Microsoft Exchange-Version ■ AV-Inhalt – Lizenzstatus
SMSMSE - Malware-Bericht	Zeigt zusammenfassende Informationen zu Malware an, die in E-Mails in Ihrer Organisation gefunden wurde. Dieser Bericht enthält die folgenden Diagramme: ■ Erste erkannte Malware ■ Erkannte Malware - Trend ■ Erste Anlagen ■ Erste Absender (eingehend/ausgehend)
SMSMSE - Absender-Drilldown-Bericht	Zeigt zusammenfassende Informationen zu E-Mails an, die von einem bestimmten E-Mail-Benutzerkonto gesendet wurden. Auf diesen Bericht greifen Sie normalerweise zu, indem Sie in einem anderen Bericht einen Drilldown in einer Liste von Absendern durchführen. Sie können jedoch auch direkt auf diesen Bericht zugreifen, indem Sie den Namen des Absenders eingeben, den Sie anzeigen möchten. Dieser Bericht enthält die folgenden Diagramme: ■ Gesendete Malware ■ Inhaltsverletzungen ■ Verletzungstypen ■ Verletzungsdetails

Berichtsname	Beschreibung
SMSMSE - Server-Detailbericht	Zeigt zusammenfassende Informationen zu den Mail Security-Servern an, die derzeit mit Protection Center integriert sind. Dieser Bericht enthält das Diagramm "Serverdetails".

Arbeiten mit Benachrichtigungen

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Benachrichtigungen](#)
- [Anzeigen und Verwalten von Benachrichtigungen](#)
- [Benachrichtigungsdetails](#)

Info zu Benachrichtigungen

Benachrichtigungen informieren Sie über wichtige Ereignisse in Protection Center und integrierten Produkten. Protection Center generiert Benachrichtigungen für alle wichtigen Ereignisse oder Aktivitäten, die in Protection Center auftreten oder in einem integrierten Produkt erkannt werden. Jede Benachrichtigung enthält folgende Informationen: Schweregrad, Zustand, Beschreibung, Erstellungszeit und zugehöriges Produkt.

Siehe ["Anzeigen und Verwalten von Benachrichtigungen"](#) auf Seite 148.

Das Protection Center-Dashboard enthält einen Newsfeed, der die wichtigsten bzw. neuesten Benachrichtigungen anzeigt. Diese Benachrichtigungen warnen vor Problemen, die Sie beheben müssen. Beispielsweise müssen Sie ein neues Produkt hinzufügen, Informationen zu den neuesten Sicherheitsbedrohungen sammeln oder aufgrund eines Sicherheitsereignisses Änderungen vornehmen.

Siehe ["Info zum Protection Center-Dashboard"](#) auf Seite 129.

Der Benachrichtigungsschweregrad gibt die Dringlichkeit einer Benachrichtigung an: Kritisch, Warnung oder Information. Die Leiste "Benachrichtigungsübersicht" in der Protection Center-Fußzeile zeigt die Anzahl ungelöster Benachrichtigungen an. Wenn es keine ungelösten Benachrichtigungen eines bestimmten Schweregrads

gibt, wird das entsprechende Symbol ausgeblendet. Das Benachrichtigungsschweregradsymbol blinkt, wenn sich die Anzahl der Benachrichtigungen dieses Schweregrads ändert. Sie können auf ein Benachrichtigungsschweregradsymbol klicken, um den Bericht "Benachrichtigungen" zu öffnen und eine Übersicht über alle Benachrichtigungen dieses Schweregrads anzuzeigen.

Benachrichtigungen werden in Kategorien gruppiert, die den enthaltenen Datentyp (z. B. "Anwendungsdaten", "Protection Center-Leistung" und "Protection Center-Sicherheitssperre") angeben. Anhand der Kategorien können Sie Benachrichtigungen sortieren, damit Sie die Benachrichtigungen leicht finden können, die für Sie interessant sind.

Anzeigen und Verwalten von Benachrichtigungen

Der Bericht "Benachrichtigungen" zeigt Einzelheiten der Benachrichtigungen an, die Protection Center erhalten hat. Sie können den Bericht "Benachrichtigungen" verwenden, um Protection Center-Benachrichtigungen anzuzeigen und zu verwalten. Sie können die Liste der Benachrichtigungen nach Schweregrad filtern. Das Filtern nach Datum oder Zeitraum ist nicht möglich. Sie können die Daten nach einer bestimmten Spalte sortieren und die Spaltreihenfolge ändern. Sie können ausführliche Information über jede Benachrichtigung anzeigen und ggf. den Benachrichtigungszustand ändern. Wenn Sie den Bericht aktualisieren, werden die Filter- und Datensortierungseinstellungen beibehalten, aber die Spaltreihenfolge wird auf die Standardeinstellung zurückgesetzt.

Siehe ["Info zu Benachrichtigungen"](#) auf Seite 147.

Der Benachrichtigungszustand gibt an, welche Benachrichtigungen neu, bestätigt oder gelöst sind. Wenn eine Benachrichtigung erzeugt wird, wird der Zustand auf "Keine" festgelegt. Sie können den Zustand einer Benachrichtigung auf "Bestätigt" festlegen, um darauf hinzuweisen, dass Sie die Benachrichtigung gelesen aber noch nicht gelöst haben. Die Anzahl neuer und bestätigter Benachrichtigungen wird addiert, um die Anzahl der Benachrichtigungen jedes Typs zu erhalten, die in der Benachrichtigungsübersicht angezeigt wird. Sie legen den Benachrichtigungszustand auf "Gelöst" fest, wenn Sie die entsprechenden Aktionen zum Lösen des Problems ausgeführt haben. Gelöste Benachrichtigungen werden aus der Benachrichtigungsübersicht entfernt. Jedoch werden sie nicht aus dem Bericht "Benachrichtigungen" entfernt.

So zeigen Sie Benachrichtigungen an

1 In Protection Center haben Sie folgende Möglichkeiten:

So zeigen Sie alle Benachrichtigungen an

- Klicken Sie im Navigationsbereich auf "Berichte".
- Klicken Sie im linken Teilfenster in der Liste "Berichte" auf "Benachrichtigungen".

So zeigen Sie die Benachrichtigungen eines bestimmten Schweregrads an

Klicken Sie unten links im Bereich "Benachrichtigungsübersicht" Sie auf das Symbol für den gewünschten Schweregrad:

- Kritisch
- Warnung
- Information

- 2 (Optional) Legen Sie in der Kopfzeile des Berichts "Benachrichtigungen" den anzuwendenden Filter "Warnmeldungsschweregrad" fest.

Siehe ["Anwenden von Filtern auf einen Bericht"](#) auf Seite 138.

So zeigen Sie ausführliche Information über eine Benachrichtigung an

- ◆ Im Bericht "Benachrichtigungen" klicken Sie auf die Benachrichtigung, die Sie anzeigen möchten.

Die Details der Benachrichtigung werden unter "Details" angezeigt.

Siehe ["Benachrichtigungsdetails"](#) auf Seite 149.

So ändern Sie den Zustand einer Benachrichtigung

- 1 Im Bericht "Benachrichtigungen" klicken Sie auf die zu ändernde Benachrichtigung.
- 2 Sie haben folgende Möglichkeiten:

So ändern Sie den Benachrichtigungszustand in "Bestätigt"

Klicken Sie auf "Bestätigen".

So ändern Sie den Benachrichtigungszustand in "Gelöst"

Klicken Sie auf "Lösen".

Benachrichtigungsdetails

Der Abschnitt "Details" des Berichts "Benachrichtigungen" enthält die ausführlichen Informationen, die für die ausgewählte Benachrichtigung verfügbar sind.

Siehe ["Anzeigen und Verwalten von Benachrichtigungen"](#) auf Seite 148.

Tabelle 14-1 Benachrichtigungsdetails

Element	Beschreibung
Schweregrad	Gibt die Dringlichkeit der Benachrichtigung an. Die verfügbaren Schweregradeinstellungen lauten wie folgt: ■ "Kritisch" - schwerwiegende Probleme, die für das Funktionieren von Protection Center kritisch sind. Beispiele für kritische Probleme sind volle Datenträger und Anwendungskomponenten, die nicht richtig funktionieren. ■ "Warnung" - Probleme, die nicht schwerwiegend sind, aber überwacht oder untersucht werden müssen. Beispiele für Probleme, die zu Warnungen führen, sind fehlgeschlagene Authentifizierungsversuche und Berichtsprobleme, die Aufmerksamkeit erfordern. ■ "Information" - Benachrichtigungen zu geringfügigen Problemen in Protection Center.
Status	Zeigt den aktuellen Status der Benachrichtigung an. Die möglichen Status lauten wie folgt: ■ "Keine" - der erste Status für alle neu generierten Benachrichtigungen. ■ "Bestätigt" - der Benutzer hat die Benachrichtigung erhalten und bestätigt, aber das Problem ist noch nicht gelöst. ■ "Geklärt" - das Problem, das die Benachrichtigung verursacht hat, ist gelöst.
Host	Gibt den Namen oder die IP-Adresse des Produkthosts an, der die Benachrichtigung generiert hat.
Zuerst aufgetreten Zuletzt aufgetreten	Gibt das Datum und die Uhrzeit an, zu der die Benachrichtigung zuerst und zuletzt aufgetreten ist.
Anzahl	Gibt an, wie viel Mal die Benachrichtigung insgesamt aufgetreten ist. Die Anzahl ist unabhängig von dem im Bericht "Benachrichtigungen" angegebenen Datumsbereich.
Beschreibung	Enthält eine Kurzbeschreibung der Benachrichtigung.
Kategorie	Gibt die Kategorie der Benachrichtigung an. Die gängigen Kategorien sind "Anwendungsdaten", "Leistung von Protection Center" und "Protection Center-Sicherheitssperre".
Details	Enthält eine ausführliche Beschreibung der Benachrichtigung.

Arbeiten mit Arbeitsabläufen und Aufgaben

In diesem Kapitel werden folgende Themen behandelt:

- [Info zu Workflows](#)
- [Verwendung von Protection Center-Workflows](#)
- [Konfigurieren der Verwaltungseinstellungen für einen Workflow](#)
- [Starten eines Workflows](#)
- [Überwachen Ihrer Workflows und Aufgaben](#)
- [Workflow-Details](#)
- [Aufgabendetails](#)
- [Reaktion auf eine Aufgabenzuweisung](#)
- [Verfügbare Workflows in Protection Center](#)

Info zu Workflows

Protection Center stellt Workflows bereit, um Ihr Sicherheitsmanagement zu vereinfachen und Ihnen zu helfen, eine sichere Umgebung zu erhalten. Ein Workflow ist eine Reihe von Aufgaben, die in einer vordefinierten Reihenfolge miteinander verknüpft sind, sodass ein Ziel erreicht wird. Einige Workflows werden automatisch ausgeführt, während andere zum Starten einen Benutzereingriff erfordern.

Die Aufgaben in einem Workflow sind die einzelnen Schritte, die durchgeführt werden müssen, um den Workflow abzuschließen. Die meisten Aufgaben in einem Workflow werden automatisch ohne Benutzereingriff ausgeführt. Einige Aufgaben erfordern einen Benutzereingriff. In einem solchen Fall wird die betreffende Aufgabe zum Bericht "Workflow-Status" hinzugefügt. Vom Bericht aus können Sie die notwendigen Aktionen durchführen, um die Aufgabe abzuschließen. Damit Sie Ihre Aufgaben besser nachverfolgen können, wird

Benachrichtigungsübersichtsbereich der Protection Center-Fußzeile ein Zwischenablagensymbol angezeigt, das die Anzahl Ihrer vorhandenen Aufgaben angibt. Sie können auf das Symbol klicken, um den Bericht "Workflow-Status" zu öffnen und dort die betreffenden Aufgaben anzuzeigen und zu bearbeiten.

Aufgaben können je nach Workflow-Prozess seriell oder parallel ausgeführt werden. An einigen Stellen im Workflow-Prozess müssen möglicherweise alle vorherigen Aufgaben abgeschlossen werden, bevor der Workflow fortgesetzt werden kann.

Alle Workflows sind in Protection Center enthalten. Sie werden nicht durch integrierte Produkte hinzugefügt. Einige Workflows sind auf bestimmte Produkte angewiesen und sind nur dann verfügbar, wenn diese Produkte in Protection Center integriert sind. Beispielsweise erfordern die Workflows "Endgerät verschieben", "Quarantäneendgerät", "Virendefinitionen und Scan-Endgerät aktualisieren" und "Virendefinitionen auf Endgerät aktualisieren" die Integration von Symantec Endpoint Protection.

Siehe ["Verwendung von Protection Center-Workflows"](#) auf Seite 152.

Siehe ["Verfügbare Workflows in Protection Center"](#) auf Seite 159.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

Siehe ["Überwachen Ihrer Workflows und Aufgaben"](#) auf Seite 155.

Verwendung von Protection Center-Workflows

Mit Protection Center-Workflows können Sie Aktionen auf spezifischen Endgeräten durchführen. Der Protection Center-Administrator muss jeden Workflow konfigurieren, um den Anforderungen Ihres Unternehmens zu entsprechen. Ein Sicherheitsmanager kann die Workflows dann verwenden, um alle Sicherheitsprobleme zu lösen, die in Ihrer Umgebung erkannt werden.

Siehe ["Info zu Workflows"](#) auf Seite 151.

Um einen Workflow zu verwenden, wählen Sie das entsprechende Endgerät in einem Bericht und dann die Aktion aus, die Sie durchführen möchten. Protection

Center beginnt mit dem entsprechenden Workflow. Sie können den Status der Workflows überwachen, die Sie begannen. Sie können außerdem die auszuführenden Aufgaben anzeigen und Aktionen bei den Aufgaben ausführen, die Ihnen zugewiesen werden.

Die folgende Tabelle beschreibt den Prozess für die Anwendung von Workflows in Protection Center.

Tabelle 15-1 Prozess für die Anwendung von Protection Center-Workflows

Schritt	Aufgabe	Beschreibung
Schritt 1	Konfigurieren Sie die Workflow-Verwaltungseinstellungen.	Jeder Workflow umfasst mindestens eine konfigurierbare Einstellung. Bevor Sie einen Workflow verwenden können, müssen Sie seine Verwaltungseinstellungen konfigurieren, um ihn den Anforderungen Ihres Unternehmens anzupassen. Siehe " Konfigurieren der Verwaltungseinstellungen für einen Workflow " auf Seite 154.
Schritt 2	Workflows beginnen	Wenn Sie eine Aktion in einem Bericht auswählen, beginnt Protection Center mit dem entsprechenden Workflow auf dem entsprechenden Endgerät. Für die meisten Workflows müssen Sie die relevanten Aktionseinstellungen festlegen, wie zum Beispiel die Workflow-Aufgaben den entsprechenden Protection Center-Benutzern zuzuweisen. Siehe " Starten eines Workflows " auf Seite 154.
Schritt 3	Zeigen Sie den Workflow-Status an.	Der Workflow-Status -Bericht zeigt Einzelheiten aller Workflows an, die innerhalb eines angegebenen Datumsbereichs begonnen wurden. Sie können den Status der Workflows überwachen, die Sie begannen. Siehe " Überwachen Ihrer Workflows und Aufgaben " auf Seite 155.
Schritt 4	Bearbeiten Sie die Ihnen zugewiesenen Aufgaben.	Die Ansicht "Workflow-Status" -Bericht ermöglicht es Ihnen, die von Ihnen durchzuführenden Aufgaben anzuzeigen. Sie können die entsprechenden Aktionen auswählen, um die Aufgaben abzuschließen, die Ihnen zugewiesen werden. Siehe " Reaktion auf eine Aufgabenzuweisung " auf Seite 158.
Schritt 5	Fehlerbehebung bei Workflows-Fehlern	Wenn ein Workflow nicht richtig funktioniert, wird eine E-Mail, zum entsprechenden Workflow-Anwender geschickt. Siehe " Ressourcen zur Problembehebung in Protection Center " auf Seite 113.

Konfigurieren der Verwaltungseinstellungen für einen Workflow

Jeder Protection Center-Workflow umfasst mindestens eine konfigurierbare Einstellung. Beispielsweise können Sie in den meisten Workflows die E-Mail-Adresse des Workflow-Administrators angeben. Wenn der Workflow fehlschlägt, schickt Protection Center eine E-Mail mit Details zu dem Fehlschlag an den zuständigen Administrator. Bevor Sie einen Workflow verwenden können, müssen Sie seine Verwaltungseinstellungen konfigurieren, um ihn den Anforderungen Ihres Unternehmens anzupassen.

Hinweis: Ihr Protection Center-Benutzerkonto benötigt die Workflow-Berechtigung zum Konfigurieren von Verwaltungseinstellungen für einen Workflow.

Siehe ["Info zu Workflows"](#) auf Seite 151.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

So konfigurieren Sie Verwaltungseinstellungen für einen Workflow

- 1 Klicken Sie in Protection Center im Menü "Admin > Einstellungen" auf "Workflow".
- 2 In der Dropdown-Liste "Vom Benutzer bearbeitbare Workflows" wählen Sie den Workflow aus, den Sie konfigurieren möchten.
- 3 Geben Sie die entsprechenden Verwaltungseinstellungen an.
Siehe ["Verfügbare Workflows in Protection Center"](#) auf Seite 159.
- 4 Klicken Sie auf "Änderungen speichern".

Starten eines Workflows

Wenn Sie eine Aktion in einem Bericht auswählen, beginnt Protection Center mit dem entsprechenden Workflow auf dem entsprechenden Endgerät. Für die meisten Workflows müssen Sie die relevanten Aktionseinstellungen festlegen, wie zum Beispiel die Workflow-Aufgaben den entsprechenden Protection Center-Benutzern zuzuweisen.

Siehe ["Info zu Workflows"](#) auf Seite 151.

Workflows sind vom Aktionen -Menü in den relevanten Protection Center-Berichten verfügbar.

Um einen Workflow zu beginnen, müssen Sie die entsprechenden Berechtigungen für die Produkte haben, die die Workflows-Aufgaben durchführen. Wenn Sie nicht

die notwendigen Produktberechtigungen haben, schlägt der Workflow mit einem Fehler, dass kein Benutzer mit dem Produktserver verbunden ist, fehl.

Siehe "[Verfügbare Workflows in Protection Center](#)" auf Seite 159.

So beginnen Sie einen Workflow

- 1 Klicken Sie in Protection Center im Navigationsbereich auf "Berichte".
- 2 Klicken Sie im linken Teilfenster in der Berichte -Liste auf den entsprechenden Bericht.
- 3 Wählen Sie im Bericht im entsprechenden Diagramm das Endgerät aus, auf dem Sie Aktion ausführen möchten.
- 4 Klicken Sie in der oberen rechten Ecke auf "Aktionen" und dann auf den Workflow, den Sie beginnen möchten.
- 5 Im Dialogfeld "Einstellungskonfiguration" geben Sie die relevanten Aktionseinstellungen an.
- 6 Klicken Sie auf "Senden".
- 7 Wenn die Bestätigungsmeldung erscheint, klicken Sie auf "Schließen".

Überwachen Ihrer Workflows und Aufgaben

Der Workflow-Status -Bericht zeigt Einzelheiten aller Workflows an, die innerhalb eines angegebenen Datumsbereichs begonnen wurden. Sie können den Status der Workflows überwachen, die Sie begannen. Der Bericht zeigt an, welche Workflows abgeschlossen sind und zu wie viel Prozent die noch laufenden Workflows abgeschlossen sind.

Siehe "[Info zu Workflows](#)" auf Seite 151.

Im Bericht "Workflow-Status" können Sie die Aufgaben anzeigen, die ausgeführt werden müssen, und diejenigen bearbeiten, die Ihnen zugewiesen sind. Beispielsweise können Sie die Quarantäne für ein Endgerät aufheben, das zu einer Quarantänegruppe in Symantec Endpoint Protection hinzugefügt wurde. Welche Aktionen verfügbar sind, hängt davon ab, welche Aufgabe ausgewählt wurde und welche Produkte mit Protection Center integriert sind.

Die Workflows, für die keine integrierten Produkte notwendig sind, werden normalerweise im Hintergrund ausgeführt und erfordern keinen Benutzereingriff. Diese Workflows erscheinen nicht im Bericht "Workflow-Status". Beispielsweise überwachen die Workflows "NationalThreatLevelMonitor" und "ZeroDayVulnerability" Datenflüsse und senden bei Bedarf E-Mail-Warnmeldungen.

So überwachen Sie Ihre Workflows und Aufgaben

- 1
- In Protection Center haben Sie folgende Möglichkeiten:
- So zeigen Sie alle mit Ihnen verknüpften Workflows an

■ Klicken Sie im Navigationsbereich auf "Berichte".

■ Klicken Sie im linken Teilfenster in der Liste "Berichte" auf "Workflow-Status".

So zeigen Sie die Aufgaben an, die ausgeführt werden müssen

Klicken Sie unten links im Bereich "Benachrichtigungsübersicht" auf das (Zwischenablage-)Symbol "Aufgabe".
- 2
- (Optional) Geben Sie im Header des Berichts "Workflow-Status" den Zeitraum für die anzuzeigenden Workflows und Aufgaben an.

Sie können einen der vordefinierten Zeiträume auswählen oder einen benutzerdefinierten Zeitraum festlegen.
- 3
- Zeigen Sie die Workflow-Details und die Aufgabendetails an.

Siehe "Workflow-Details" auf Seite 156.

Siehe "Aufgabendetails" auf Seite 157.
- 4
- (Optional) Aktualisieren Sie den Bericht, um sicherzustellen, dass die neuesten Details angezeigt werden.

Es kann einige Minuten dauern, die Workflow-Statusinformationen zu aktualisieren.

Workflow-Details

Das Workflow-Status -Diagramm zeigt Einzelheiten der Workflows , die Sie angefangen haben und ermöglicht Ihnen die Überwachung des Status jedes Workflows.

Siehe "Überwachen Ihrer Workflows und Aufgaben" auf Seite 155.

Die folgende Tabelle beschreibt die Informationen, die im Workflow-Status -Diagramm für jeden Workflow angezeigt werden.

Tabelle 15-2 Workflow-Details

Element	Beschreibung
Prozess-ID	Gibt die Prozess-ID für den Workflow an. Mit dieser ID können Sie die Aufgaben des Workflows, die im Diagramm "Meine Aufgaben" angezeigt werden, dem Workflow zuordnen.

Element	Beschreibung
Name	Gibt den Namen des Workflows an.
Status	Gibt den Status des Workflows an. Die Statuswerte sind für jeden Workflow spezifisch. Im Allgemeinen sind die Statuswerte "Vorgang läuft", "In Bearbeitung", "Abgeschlossen" und "Fehlgeschlagen".
"Gestartet"	Gibt das Startdatum und die Startzeit des Workflows an.
"Beendet"	Gibt das Enddatum und die Endzeit des Workflows an.
% abgeschlossen	Zeigt an, wieviel Prozent des Workflows abgeschlossen sind. Jeder einzelne Workflow verwendet seine eigenen Kriterien, um anzuzeigen, wie weit der Workflow fortgeschritten ist.

Aufgabendetails

Das Diagramm "Meine Aufgaben" zeigt Einzelheiten der Aufgaben, die durchgeführt werden müssen und Sie können die entsprechende Aktionen für die Ihnen zugewiesene durchführen.

Siehe "[Überwachen Ihrer Workflows und Aufgaben](#)" auf Seite 155.

Die folgende Tabelle beschreibt die Informationen, die im Meine Aufgaben -Diagramm für jede Aufgabe angezeigt werden.

Tabelle 15-3 Aufgabendetails

Element	Beschreibung
Prozess-ID	Gibt die Prozess-ID für den übergeordneten Workflow an. Mit dieser ID können Sie die Aufgabe dem entsprechenden Workflow im Workflow-Status Diagramm zuordnen.
Aufgabenname	Gibt den Namen der Aufgabe an.
Name	Gibt den Namen des Workflow-Prozesses an, der mit der Aufgabe verknüpft ist.
"Zuweisungsdatum"	Gibt das Datum an, an dem die Aufgabe einem Benutzer zugewiesen wurde.
"Fällig am"	Gibt das Datum an, an dem die Aufgabe fällig ist.
Status	Gibt den aktuellen Status der Aufgabe an: "Offen" oder "Geschlossen".

Element	Beschreibung
"Aktionen"	Ermöglicht Ihnen, auf die Aktionen zuzugreifen, die für die Aufgabe verfügbar sind. Mit der Option "Antworten" können Sie die Aufgabe abschließen. Siehe "Reaktion auf eine Aufgabenzuweisung" auf Seite 158.

Reaktion auf eine Aufgabenzuweisung

Wenn Ihnen eine Workflow-Aufgabe zugewiesen wird, müssen Sie auf die Aufgabe reagieren und die entsprechende Aktion durchführen. Dabei müssen Sie normalerweise die Informationen bereitstellen, die erforderlich sind, um die Aufgabe abzuschließen.

Siehe ["Überwachen Ihrer Workflows und Aufgaben"](#) auf Seite 155.

So reagieren Sie auf eine Aufgabenzuweisung

- 1 In Protection Center haben Sie folgende Möglichkeiten:
 - Klicken Sie im Navigationsbereich auf "Berichte" und dann in der Liste "Berichte" auf "Workflow-Status".
 - Im Bereich "Benachrichtigungsübersicht" klicken Sie auf das Symbol "Aufgabe" (Zwischenablage).
- 2 Im Bericht "Workflow-Status" klicken Sie im Diagramm "Meine Aufgaben" auf die Aufgabe, die Sie erledigen möchten.
- 3 Klicken Sie auf "Aktionen" und dann auf "Antworten".
- 4 Im Dialogfeld "Aktion für Antwort" führen Sie die Aktionen durch, die notwendig sind, um die Aufgabe abzuschließen.

Welche Aktionen Sie durchführen müssen, hängt von der Aufgabe ab, auf die Sie reagieren.

Siehe ["Verfügbare Workflows in Protection Center"](#) auf Seite 159.

- 5 (Optional) wenn Sie die Aufgabe schließen möchten, ohne irgendwelche Aktionen durchzuführen, klicken Sie auf "Aufgabe schließen/Vorgang abschließen".

Sie müssen eine Aufgabe schließen, wenn die Aufgabenaktionen bereits außerhalb der Protection Center-Umgebung durchgeführt worden sind.

Wenn z. B. ein Endgerät aus einer Quarantänegruppe innerhalb Symantec Endpoint Protection heraus verschoben wird, bleibt die entsprechende Aufgabe "Handle Unquarantined Machine" in Protection Center möglicherweise geöffnet. Sie müssen die Aufgabe schließen, ohne eine weitere Aktion durchzuführen.

- 6 Klicken Sie auf "Schließen".

Verfügbare Workflows in Protection Center

Alle Workflows sind in Protection Center enthalten. Sie werden nicht durch integrierte Produkte hinzugefügt. Einige Workflows sind auf bestimmte Produkte angewiesen und sind nur dann verfügbar, wenn diese Produkte in Protection Center integriert sind.

Siehe ["Info zu Workflows"](#) auf Seite 151.

Tabelle 15-4 Verfügbare Workflows in Protection Center

Workflow	Erforderliches Produkt	Beschreibung
"Endgerät verschieben"	Symantec Endpoint Protection	Verschiebt das ausgewählte Endgerät in eine andere Gruppe im Symantec Endpoint Protection Manager. Dieser Workflow ist im Spezifische Malware -Bericht verfügbar. Der Aktionsname ist "In eine andere SEP-Gruppe verschieben". Siehe "Workflow "Endgerät verschieben" " auf Seite 164.
Quarantäneendgerät	Symantec Endpoint Protection	Verschiebt das ausgewählte Endgerät in eine spezifische Gruppe im Symantec Endpoint Protection Manager. Der Workflow weist auch die entsprechende Aufgabe zum Aufheben der Isolierung einem angegebenen Benutzer zu. Dieser Workflow ist im Spezifische Malware -Bericht verfügbar. Der Aktionsname ist "Mit SEP isolieren". Siehe "Quarantäneendgerät -Workflow" auf Seite 161.

Workflow	Erforderliches Produkt	Beschreibung
"Virendefinitionen und Scan-Endgerät aktualisieren"	Symantec Endpoint Protection	Aktualisiert die Virendefinitionen auf dem ausgewählten Endgerät und führt dann einen Virenskan auf diesem Endgerät durch. Dieser Workflow ist im Spezifische Malware -Bericht verfügbar. Der Aktionsname ist "Definitionen aktualisieren und scannen". Siehe "Workflow "Virendefinitionen und Scan-Endgerät aktualisieren"" auf Seite 164.
"Virendefinitionen auf Endgerät aktualisieren"	Symantec Endpoint Protection	Aktualisiert die Virendefinitionen auf dem ausgewählten Endgerät. Dieser Workflow ist im Spezifische Malware -Bericht verfügbar. Der Aktionsname ist "Definitionen aktualisieren". Dieser Workflow ist auch im Bestimmtes Endgerät -Bericht über die Schaltfläche "Definitionen aktualisieren" verfügbar. Siehe "Workflow "Virendefinitionen auf Endgerät aktualisieren"" auf Seite 163.
"NationalThreatLevelMonitor"	Keine	Überwacht den "NationalThreatLevelMonitor" -Datenfluss. Wenn sich die Bedrohungsstufe ändert, schickt der Workflow eine E-Mail an den Benutzer, der in den Workflow-Einstellungen angegeben ist. Dieser Workflow wird im Hintergrund ausgeführt und erscheint nicht im Workflow-Status -Bericht. Sie können ihn nicht manuell beginnen. Siehe """NationalThreatLevelMonitor" -Workflow"" auf Seite 165.
"ZeroDayVulnerabilityMonitor"	Keine	Überwacht den "ZeroDayVulnerabilityMonitor" -Datenfluss. Wenn eine neue Infektion erkannt wird, schickt der Workflow eine E-Mail an den Benutzer, der in den Workflow-Einstellungen angegeben ist. Dieser Workflow wird im Hintergrund ausgeführt und erscheint nicht im Workflow-Status -Bericht. Sie können ihn nicht manuell beginnen. Siehe """ZeroDayVulnerabilityMonitor" -Workflow"" auf Seite 166.

Quarantäneendgerät -Workflow

Der "Quarantäneendgerät" -Workflow verschiebt das ausgewählte Endgerät in die angegebene Gruppe innerhalb des Symantec Endpoint Protection Managers. Er erstellt auch eine entsprechende Aufgabe zum Aufheben der Isolierung. Der zugewiesene Benutzer muss dann das Problem auf dem Endgerät lösen. Wenn das Problem gelöst wird, kann der Benutzer auf die Aufgabe reagieren und das Endgerät zurück in die ursprünglichen Gruppe verschieben. Wenn das Endgerät erfolgreich verschoben wird, wird die Aufgabe geschlossen und als abgeschlossen markiert.

Dieser Workflow ist nur verfügbar, wenn Symantec Endpoint Protection in Protection Center integriert ist.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Warnung: Wenn das Endgerät zu Beginn des Workflows bereits in der ausgewählten Quarantänegruppe ist, wird die Aufgabe zum Aufheben der Isolierung nicht erstellt. Eine entsprechende Benachrichtigung wird im "Benachrichtigungen" -Bericht angezeigt.

Der Benutzer, dem die Aufgabe zum Aufheben der Isolierung zugewiesen wird, muss eine Benutzerberechtigung in Symantec Endpoint Protection haben, einen Client zu verschieben. Falls dies nicht der Fall ist, wird der Schritt zum Aufheben der Isolierung innerhalb des Workflow nicht durchgeführt und eine Fehlermeldung ausgelöst.

Tabelle 15-5 Verwaltungseinstellungen für Quarantäneendgerät -Workflow

Einstellung	Beschreibung
Is Using Task Alert Emails	Legt fest, dass der Workflow Warnmeldungs-E-Mails zum Aufgabenbesitzer schickt.
Hours To Wait For Assignee To Work Task	Legt den Zeitraum fest, in dem der Workflow auf den zugewiesenen Aufgabenbesitzer wartet, um die entsprechende Aktion zu beginnen. Die Aufgabe funktioniert nicht, wenn die angegebene Wartezeit überschritten wird. Der "Workflow-Status" -Bericht wird aktualisiert, um den Aufgabenstatus als fehlgeschlagen anzuzeigen. Protection Center schickt auch eine Benachrichtigung zum Newsfeed im Protection Center-Dashboard.
Workflow Owner Email	Gibt die E-Mail-Adresse des Protection Center-Workflow-Administrators an. Wenn der Workflow fehlschlägt, schickt Protection Center Informationen zu diesem Problem an den Workflow-Administrator.

Der "Quarantäneendgerät" -Workflow ist im "Spezifische Malware" -Bericht, durch die "Mit SEP isolieren" Aktion verfügbar.

Das Dialogfeld "Aktion für Mit SEP isolieren" erscheint, wenn Sie den "Quarantäneendgerät" -Workflow beginnen. Dieses Dialogfeld ermöglicht es, die Quarantänegruppe anzugeben, zu der das ausgewählte Endgerät hinzugefügt wird. Damit kann auch die passende "Handle Unquarantined Machines" -Aufgabe dem entsprechenden Protection Center-Benutzer zugewiesen werden.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

Tabelle 15-6 "Mit SEP isolieren" -Aktionseinstellungen

Einstellung	Beschreibung
Gruppenauswahl	Gibt die Quarantänegruppe an, zu der das Endgerät hinzugefügt wird.
Einem Benutzer zuweisen	Gibt den Protection Center-Benutzer an, dem die "Handle Unquarantined Machines" -Aufgabe zugewiesen ist. Der Benutzer, dem die "Handle Unquarantined Machines" -Aufgabe zugewiesen wird, muss eine Benutzerberechtigung in Symantec Endpoint Protection haben, einen Client zu verschieben.

Das Dialogfeld "Aktion für Antworten" erscheint, wenn Sie auf eine "Handle Unquarantined Machines" -Aufgabe reagieren. Dieses Dialogfeld bestätigt, dass Sie das angegebene Endgerät aus der Quarantäne entfernen und die Aufgabe schließen möchten.

Siehe ["Reaktion auf eine Aufgabenzuweisung"](#) auf Seite 158.

Die folgende Tabelle beschreibt die Einstellungen, die Sie für eine "Handle Unquarantined Machines" -Aufgabe durchführen können.

Tabelle 15-7 "Handle Unquarantined Machines" -Aufgabeneinstellungen

Einstellung	Beschreibung
"Isolierte Computer"	Zeigt das isolierte Endgerät an und sie können angeben, dass Sie die Isolierung aufheben möchten.
"Isolierung aufheben"	Gibt an, dass das ausgewählte Endgerät aus der Quarantänegruppe entfernt wird und zurück in seine ursprüngliche Gruppe gelegt wird.
"Aufgabe schließen/Vorgang abschließen"	Gibt an, dass die Aufgabe abgeschlossen. Wenn ein isoliertes Endgerät aus der Quarantänegruppe innerhalb Symantec Endpoint Protections verschoben wird, kann die entsprechende Aufgabe in Protection Center möglicherweise geöffnet bleiben. Sie müssen die Aufgabe "Handle Unquarantined Machine" schließen, ohne eine weitere Aktion anzufangen.

Workflow "Virendefinitionen auf Endgerät aktualisieren"

Der Workflow "Virendefinitionen auf Endgerät aktualisieren" aktualisiert die Virendefinitionen auf dem ausgewählten Endgerät. Keine weitere Aktion ist erforderlich.

Dieser Workflow ist nur verfügbar, wenn Symantec Endpoint Protection in Protection Center integriert ist.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Tabelle 15-8 "Virendefinitionen auf Endgerät aktualisieren" – Workflow-Verwaltungseinstellungen

Einstellung	Beschreibung
Wartezeit (Stunden) für Befehlsausführung	Gibt an, wie lange der Workflow darauf wartet, dass Symantec Endpoint Protection Manager den Abschluss der Aktion bestätigt. Der Workflow schlägt fehl, wenn die angegebene Wartezeit überschritten wird. Der Bericht "Workflow-Status" wird aktualisiert und der Workflow-Status "Fehlgeschlagen" wird angezeigt. Protection Center schickt auch eine Benachrichtigung zum Newsfeed im Protection Center-Dashboard. Das Fehlschlagen des Vorgangs bedeutet, dass der Befehl nicht innerhalb der angegebenen Zeit abgeschlossen wurde. Es ist jedoch möglich, dass der Befehl nach wie vor auf dem Symantec Endpoint Protection Manager-Server ausgeführt wird. Überprüfen Sie den Status der angesteuerten Endgeräte, bevor Sie weitere Maßnahmen ergreifen.
Workflow Owner Email	Gibt die E-Mail-Adresse des Protection Center-Workflow-Administrators an. Wenn der Workflow fehlschlägt, schickt Protection Center Informationen zu diesem Problem an den Workflow-Administrator.

Der Workflow "Virendefinitionen auf Endgerät aktualisieren" steht im Bericht "Bestimmte Malware" über die Aktion "Definitionen aktualisieren" zur Verfügung. Dieser Workflow ist auch im Bestimmtes Endgerät -Bericht über die Schaltfläche "Definitionen aktualisieren" verfügbar.

Das Dialogfeld "Aktion für Definitionen aktualisieren" erscheint, wenn Sie den Workflow "Virendefinitionen auf Endgerät aktualisieren" beginnen. Mit diesem Dialogfeld können Sie bestätigen, dass das richtige Endgerät ausgewählt ist. Der Name und die IP-Adresse des ausgewählten Endgeräts werden angezeigt. Sie brauchen, keine weiteren Aktionseinstellungen anzugeben.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

Workflow "Endgerät verschieben"

Der Workflow "Endgerät verschieben" verschiebt das ausgewählte Endgerät auf die angegebene Gruppe. Keine weitere Aktion ist erforderlich.

Dieser Workflow ist nur verfügbar, wenn Symantec Endpoint Protection in Protection Center integriert ist.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Tabelle 15-9 Workflow "Endgerät verschieben", Verwaltungseinstellungen

Einstellung	Beschreibung
Workflow Owner Email	Gibt die E-Mail-Adresse des Protection Center-Workflow-Administrators an. Wenn der Workflow fehlschlägt, schickt Protection Center Informationen zu diesem Problem an den Workflow-Administrator.

Der Workflow "Endgerät verschieben" ist im Bestimmte Malware -Bericht, durch die Aktion "In eine andere SEP-Gruppe verschieben" verfügbar.

Das Dialogfeld "Aktion für In eine andere SEP-Gruppe verschieben" erscheint, wenn Sie den Workflow "Endgerät verschieben" beginnen. Mit diesem Dialogfeld können Sie die Gruppe angeben, in die das Endgerät verschoben wird.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

Tabelle 15-10 "In eine andere SEP-Gruppe verschieben", Aktionseinstellungen

Einstellung	Beschreibung
Gruppenauswahl	Gibt die Quarantänegruppe an, in die das Endgerät verschoben wird.

Workflow "Virendefinitionen und Scan-Endgerät aktualisieren"

Der Workflow "Virendefinitionen und Scan-Endgerät aktualisieren" aktualisiert die Virendefinitionen auf dem ausgewählten Endgerät und initiiert dann einen Virensan auf dem Endgerät. Keine weitere Aktion ist erforderlich.

Dieser Workflow ist nur verfügbar, wenn Symantec Endpoint Protection in Protection Center integriert ist.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Tabelle 15-11 Administrationseinstellungen für Workflow "Virendefinitionen und Scan-Endgerät aktualisieren"

Einstellung	Beschreibung
Hours To Wait For Command To Finish	Gibt an, wie lange der Workflow darauf wartet, dass Symantec Endpoint Protection Manager den Abschluss der Aktion bestätigt. Der Workflow schlägt fehl, wenn die angegebene Wartezeit überschritten wird. Der Bericht "Workflow-Status" wird aktualisiert und der Workflow-Status "Fehlgeschlagen" wird angezeigt. Protection Center schickt auch eine Benachrichtigung zum Newsfeed im Protection Center-Dashboard. Das Fehlschlagen des Vorgangs bedeutet, dass der Befehl nicht innerhalb der angegebenen Zeit abgeschlossen wurde. Es ist jedoch möglich, dass der Befehl nach wie vor auf dem Symantec Endpoint Protection Manager-Server ausgeführt wird. Überprüfen Sie den Status der angesteuerten Endgeräte, bevor Sie weitere Maßnahmen ergreifen.
Workflow Owner Email	Gibt die E-Mail-Adresse des Protection Center-Workflow-Administrators an. Wenn der Workflow fehlschlägt, schickt Protection Center Informationen zu diesem Problem an den Workflow-Administrator.

Der Workflow "Virendefinitionen und Scan-Endgerät aktualisieren" steht im Bericht "Bestimmte Malware" (Aktion "Definitionen aktualisieren und scannen") zur Verfügung.

Das Dialogfeld "Aktion für Definitionen aktualisieren und scannen" erscheint, wenn Sie den Workflow "Virendefinitionen und Scan-Endgerät aktualisieren" beginnen. In diesem Dialogfeld geben Sie den Typ des Virenskans an, der auf dem Endgerät durchgeführt werden soll.

Siehe ["Starten eines Workflows"](#) auf Seite 154.

Tabelle 15-12 Einstellungen für Aktion "Definitionen aktualisieren und scannen"

Einstellung	Beschreibung
Scantyp	Gibt den Typ des Virenskans an, der auf dem Endgerät durchgeführt werden soll: ■ Schnellprüfung Scannt nur die am häufigsten infizierten Bereiche. ■ Vollständiger Scan Scannt den gesamten Computer.

"NationalThreatLevelMonitor" -Workflow

Der "NationalThreatLevelMonitor" -Workflow überwacht den "NationalThreatLevel" -Datenfluss. Wenn sich die Bedrohungsstufe ändert, schickt

der Workflow eine E-Mail-Warnmeldung an den angegebenen Administrator. Er wird im Hintergrund ausgeführt und eine Benutzeraktion ist nicht erforderlich.

Dieser Workflow befindet sich in Protection Center.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Tabelle 15-13 "NationalThreatLevelMonitor" -Workflow-Verwaltungseinstellungen

Einstellung	Beschreibung
"Alert To Email Address"	Gibt die E-Mail-Adresse an, an die "NationalThreatLevel" Warnmeldungen sendet.

"ZeroDayVulnerabilityMonitor" -Workflow

Der "ZeroDayVulnerabilityMonitor" -Workflow überwacht den "ZeroDayVulnerability" -Datenfluss. Wenn eine neue Infektion erkannt wird, schickt der Workflow eine E-Mail-Warnmeldung an den angegebenen Administrator. Er wird im Hintergrund ausgeführt und eine Benutzeraktion ist nicht erforderlich.

Dieser Workflow befindet sich in Protection Center.

Siehe ["Konfigurieren der Verwaltungseinstellungen für einen Workflow"](#) auf Seite 154.

Tabelle 15-14 "ZeroDayVulnerabilityMonitor" -Workflow-Verwaltungseinstellungen

Einstellung	Beschreibung
"Feed URL"	Gibt die URL des "ZeroDayVulnerability" -Datenflusses an. Der Standard ist http://static.nvd.nist.gov/feeds/xml/cve/nvdcve-2.0-modified.xml
"Alert To Email Address"	Gibt die E-Mail-Adresse an, an die "ZeroDayVulnerability" Warnmeldungen sendet.

Index

A

Active Directory

- Authentifizierungseinstellungen 70
- Basis-DN, angeben 61
- Benutzerkontoauthentifizierung 58
- Filter für die Benutzersuche, angeben 62
- Protection Center-Benutzerkonto erstellen 64
- Servereinstellungen, angeben 59

Administrator

- Benutzerkontokennwort ändern 21
- erste Aufgabeneinstellungen 20
- Info 17
- Infos zu Administratöraufgaben 25
- Optionen des ersten Einrichtens 20
- Protection Center herunterfahren 28
- Rollendefinition 25
- zugreifen auf Protection Center 18

Aktion

- "Definitionen aktualisieren", Beschreibung 163
- "Definitionen aktualisieren", Einstellungen 163
- "In eine andere SEP-Gruppe verschieben",
Beschreibung 164
- "In eine andere SEP-Gruppe verschieben",
Einstellungen 164
- "Mit SEP isolieren"-Beschreibung 161
- Definitionen aktualisieren und scannen,
Beschreibung 164
- Definitionen aktualisieren und scannen,
Einstellungen 165
- Mit SEP isolieren, Einstellungen 162

Aufgabe

- "Aktion für Antworten"-Einstellungen 162
- abschließen 162
- Aktionen 155
- Anzeigen 155
- Details 157
- Handle Unquarantined Machines 162
- Info 151
- Reaktion auf zugewiesene 158
- verwalten 155

B

Backup

- automatische planen 85
- Backup-Datei-Kennwortschutz 86
- Backup-Dateispeicherort 86
- Backup-Zeitplaneinstellungen 87
- Einstellungen angeben 85
- Image 84
- Info 84
- Info zu Einstellungen 85
- inkrementell 84
- vollständig 84
- wiederherstellen 87

Backup Exec System Recovery. *Siehe* Backup

Benachrichtigung

- Anzahl im Bericht 150
- ausführliche Beschreibung 150
- ausführliche Informationen 149
- Beschreibung im Bericht 150
- Host 150
- in Bericht anzeigen 148
- in Bericht filtern 148
- Info 147
- Information 150
- Kategorien 150
- kritisch 150
- Schweregrad, anzeigen 148
- Schweregradeinstellungen 150
- Statusereinstellungen 150
- Warnung 150
- Zustand, ändern 148
- Zustand, anzeigen 148

Benutzerberechtigungseinstellungen

Info 70

Benutzerkonto

- Active Directory- und
LDAP-Authentifizierungseinstellungen 70
- Active Directory-Konto zur Authentifizierung
auswählen 70
- Aktivieren 66
- Ändern 66

- Authentifizierungsmethode 56
- Bearbeiten 66
- Benutzerauthentifizierungstypen 67
- Benutzerberechtigungen 71
- Benutzerberechtigungseinstellungen 70
- Benutzername 56, 69
- Berechtigungen 56
- deaktivieren 66, 69
- E-Mail-Adresse 69
- erstellen 64
- Info 56
- Kennwort ändern 21
- Kennwordeinstellung 69
- Kennwortkomplexitätsanforderungen 21, 69, 109
- LDAP-Authentifizierung 68
- LDAP-Konto zur Authentifizierung
 - auswählen 70
- Lokale Authentifizierungseinstellungen 68
- Löschen 76
- Microsoft Active Directory-Authentifizierung 68
- Produktzugriffsberechtigungseinstellungen 75
- Prozess für das Konfigurieren 57
- SPC_Admin-Konto 57
- Standardadministratorkonto 56–57
- Über lokale Authentifizierung 68
- Übersicht anzeigen 63
- verknüpftes Benutzerkonto auf Produkthost 75
- verwalten 63
- zugängliche Produkte 56
- Benutzeroberfläche
 - ausloggen 22
 - einloggen 18
 - zugreifen 18
- Bereinigen. *Siehe* Datenbereinigungseinstellungen
- Bericht
 - Aktionen 135
 - Anzeigen 136
 - ausführliche Berichte anzeigen 136
 - Bearbeiten 141
 - Benachrichtigungen, anzeigen 148
 - Benachrichtigungen, ausführliche Informationen 149
 - Benachrichtigungen, Übersicht 148
 - Beschreibung, ändern 143
 - Besitzer 143
 - Diagramm 134
 - Drilldown-Berichte 136
 - Eigenschaften 142

- Einstellungen zur E-Mail-Verteilung 143
- erforderliche Parameter, angeben 136
- Ergebnisse per E-Mail verteilen 141
- Filter, anwenden 138
- Filter, benutzerdefinierte Werte 138
- Filter, durchsuchte Werte 138
- Filter, entfernen 138
- Filter, Info 135
- Filter, vordefinierte Zeiträume 136
- Filtereinstellungen, speichern 139
- Filterparameter 135
- gespeicherter Bericht, erstellen 139
- Info 134
- Löschen 141
- Name, ändern 142
- per E-Mail verteilen 141
- Planen 141
- Verteilung, ändern 143
- Verteilungsformateinstellungen 143
- Verteilungshäufigkeitseinstellungen 143
- verwalten 141
- Verwaltungseinstellungen 142
- Workflow, beginnend 135
- Zu verwendender Prozess 136

C

- Community-Statistik
 - Einstellungen konfigurieren 96
 - Info zu Einstellungen 96

D

- Dashboard
 - DeepSight-Status-Diagramm 130
 - Info 129
 - Newsfeed-Diagramm 130
 - Produktintegrationstatus-Diagramm 130
 - Produktserversstatus-Diagramm 130
 - Schutzüberblick-Diagramm 129
 - Systemstatus-Diagramm 130
 - Threatcon-Status-Diagramm 130
 - Unternehmensbedrohungen-Diagramm 131

Daten

- aus Backups wiederherstellen 87
- automatische Backups planen 85
- Diagramm 134
- in Protection Center sichern 84

Datenbereinigung

- Datentypen der bereinigten Einstellungen 102

- Einstellung planen 103
- Info zu Einstellungen 102
- Speicherplatzeinstellungen 102
- Sperrfristeinstellung 102
- unmittelbare Einstellung 103
- Datum und Uhrzeit
 - aktuelle Zeiteinstellung 97
 - Einstellungen konfigurieren 97
 - Info zu Einstellungen 97
 - Zeitzoneneinstellung 97
- DeepSight
 - Info 129
- Diagnosedaten
 - Diagnosedatei an den Symantec-Support
 - senden 123
 - Diagnosedatei-Übertragungsdetails 118
 - Diagnosedatei-Übertragungseinstellungen 122
 - Diagnosedatensammlungsergebnisse 118
 - Diagnoseergebnisdatei speichern 122
 - Diagnosekonfigurationsdatei 121
 - Kundenservice-Fall-ID 118, 120
 - Ressourcen zum Beheben von Problemen 113
 - sammeln 115, 118
 - Support-Diagnoseeinstellungen 116
 - Supportanfrage erstellen 118
 - Supportanfrageneinstellungen 120
- Diagramm
 - in Berichten verwendete Typen 134
 - Info 134
- DNS
 - Adresse, alternativer Server 100
 - Adresse, Primärserver 100
 - IPv4- oder IPv6-Netzwerkeinstellungen
 - angeben 109

E

- E-Mail
 - Administrator-Adresseinstellungen 97
 - E-Mail-Servereinstellungen 97
 - Einstellungen konfigurieren 97
 - Info zu Einstellungen 97
- E-Mail-Einstellungen
 - Absenderadresse 98
 - SMTP-Server-Port 98
 - SMTP-Servername 98
 - Zieladresse 98
- Einstellungen
 - "Active Directory und LDAP"-Server 59

- Active Directory- und
 - LDAP-Authentifizierung 70
- Authentifizierung Protection Center (lokal) 68
- Backup 85
- Berichtsverteilung 143
- Berichtsverwaltung 142
- Community-Statistik 96
 - Siehe auch* Community-Statistik
- Datenbereinigung 102
 - Siehe auch* Datenbereinigung
- Datum und Uhrzeit 97
 - Siehe auch* Datum und Uhrzeit
- E-Mail-Server 97
 - Siehe auch* E-Mail
- erforderlich für unterstützten Produkthost 33
- Erweiterter unterstützter Produkthost 33
- in der Benutzeroberfläche zugreifen 96
- LiveUpdate 81
- Nachrichtenprotokollierung 99
 - Siehe auch* Nachrichtenprotokollierung
- Netzwerkkonfiguration 100
 - Siehe auch* Netzwerk
- Produktzugriffsberechtigung 75
- Protection
 - Center-Benutzerkontoberechtigungen 70
 - Protection Center-Konfiguration, Info 93
- Proxy-Server 101
 - Siehe auch* Proxy-Server
- Supportanfrage 120
- Systemsteuerung 106
 - Siehe auch* Systemsteuerung
- Verwaltung, für einen Workflow
 - konfigurieren 154
- erstes Einrichten
 - Benutzerkonten 20
 - Community-Statistik 21
 - E-Mail-Server 20
 - Info 20
 - Produkt hinzufügen 32
 - Produktintegration 20
 - Proxy-Server 21
 - Tenant des Multi-Tenant-Produkts
 - hinzufügen 32

F

- Fehlersuche
 - Diagnosedatei an den Symantec-Support
 - senden 123
 - Diagnosedatei-Übertragungsdetails 118

- Diagnosedatei-Übertragungseinstellungen 122
- Diagnosedaten sammeln 115, 118
- Diagnosedatensammlungsergebnisse 118
- Diagnoseergebnisdatei speichern 122
- Diagnosekonfigurationsdatei 121
- Kundenservice-Fall-ID 118, 120
- Ressourcen zum Beheben von Problemen 113
- Support-Diagnoseeinstellungen 116
- Supportanfrage erstellen 118
- Supportanfrageneinstellungen 120
- Frühwarnmeldungen. *Siehe* Global Intelligence Network
- FTP
 - Diagnosedatei-Übertragungsdetails anzeigen 116
 - Diagnosedatei-Übertragungseinstellungen angeben 120
 - zum Senden der Diagnosedatei an den Symantec-Support 123

G

- Global Intelligence Network
 - Benachrichtigungen im Newsfeed 129
 - Info 13

H

- Herunterfahren
 - Protection Center 28
- HTTP-Proxy-Server
 - festlegen 101
 - Info 101

K

- Kennwort
 - ändern 21
 - Einstellung 69
 - SPC_Admin-Konto, ändern 108

L

- LDAP
 - Authentifizierungseinstellungen 70
 - Basis-DN, angeben 61
 - Benutzerkontoauthentifizierung 58
 - Filter für die Benutzersuche, angeben 62
 - Protection Center-Benutzerkonto erstellen 64
 - Servereinstellungen, angeben 59
- LiveUpdate. *Siehe* Softwareupdate

M

- Mail Security-Integration
 - Info 41
 - Integrationsvorgang 42
 - Mail Security in Protection Center aktivieren 44
 - Mail Security-Plugin aktualisieren 51
 - Mail Security-Plugin installieren 45, 52
 - Mail Security-Plugin, Pull-Installation 48
 - Mail Security-Plugin, Push-Installation 46
 - Mail Security-Plugin-Installation überwachen 49
 - Mail Security-Plugin-Status anzeigen 49
 - repräsentative Produktinstanz 42, 44
 - spezielle Berichte für Mail Security 144
 - Statusinformationen zum Mail Security-Plugin 50
 - Statusinformationen zum Symantec Management-Agent 50
 - Symantec Management Agent, Push-Installation 46
 - Symantec Management-Agent aktualisieren 51
 - Symantec Management-Agent deinstallieren 52
 - Symantec Management-Agent installieren 45
 - Symantec Management-Agent, Pull-Installation 48
 - Symantec Management-Agent-Installation überwachen 49
 - Symantec Management-Agent-Status anzeigen 49
- Microsoft Active Directory. *Siehe* Active Directory

N

- Nachrichtenprotokollierung
 - ausführliche Protokollierungseinstellungen 99
 - Einstellungen konfigurieren 99
 - Info zu Einstellungen 99
 - normale Protokollierungseinstellungen 99
- Netzwerk
 - DNS-Servereinstellung, alternativ 100
 - DNS-Servereinstellung, primär 100
 - Einstellungen in der Systemsteuerung konfigurieren 109
 - Einstellungen konfigurieren 100
 - Info zu Einstellungen 100
 - Info zu Konfigurationseinstellungen 100
 - IP-Adresseinstellung, Appliance 100
 - Standard-Gateway-Einstellung 100
 - Subnetzmaskeneinstellung 100
 - Subnetzpräfix-Längeneinstellung 100

Neu starten
Protection Center 28

P

Produkterkennungseinstellungen
Host mit mehreren Mandanten 35
Konfigurieren 35
Protection Center
Active Directory-Einstellungen 59
aus Backup wiederherstellen 87
ausloggen 22
Benachrichtigungen. *Siehe* Benachrichtigung
Benutzerberechtigungen 71
Benutzerkonto. *Siehe* Benutzerkonto
Berichte. *Siehe* Bericht
Betriebssystem, aktivieren 111
Dashboard 129
Diagnosedaten sammeln 115
Siehe auch Diagnosedaten
einloggen 18
Erste Schritte 17
Funktionsweise 14
Geschäftsanalysen, Konfigurieren 27
Geschäftsanalysen, Überblick 27
herunterfahren 28
Info 13
Info zu Administratöraufgaben 17
Info zu Sicherheits-Manager-Aufgaben 17
Info zu unterstützten Produkten 29
Konfigurationseinstellungen. *Siehe*
Einstellungen
LDAP-Einstellungen 59
neu starten 28
Produkt aktivieren 37
Produkt deaktivieren 38
Produkt erneut aktivieren 39
Produkt hinzufügen 32
Produkt integrieren 30
Produkt verwalten 131
Produkterkennung 35
sichern 84
Siehe auch Backup
Softwarekomponenten manuell
aktualisieren 107
Softwareupdates. *Siehe* Softwareupdate
Standardadministratorkonto 56–57
Startseite. *Siehe* Dashboard
Systemsteuerung. *Siehe* Systemsteuerung

Windows Update-Server-Speicherort,
angeben 111
zusätzliche Informationen 15

Proxy-Server
Einstellungen konfigurieren 101
HTTP-Proxy-Server-Porteinstellung 101
HTTP-Proxy-Servernameneinstellung 101
Info zu Einstellungen 101

S

Sicherheits-Manager
Info zu Sicherheitsmanagement-Aufgaben 127
Rollendefinition 127
zugreifen auf Protection Center 18
Sicherheitsmanager
Benutzerkontokennwort ändern 21
Info 17
SMTP
Info 97
Server angeben 97
Softwareupdate
Anzeigen 78
auf Anforderung nach neuen Updates suchen 78
automatische Updates deaktivieren 81
Herunterladen vom LiveUpdate-Server 78
Info 77
Installieren 78
lokale LiveUpdate-Servereinstellungen 81
manuell 108
Verwendung des lokalen LiveUpdate-Server 80
Verwendung des Symantec
LiveUpdate-Servers 80
SPC_Admin-Konto
auf die Systemsteuerung zugreifen 107
Kennwort ändern 108
Startseite. *Siehe* Dashboard
Symantec Recovery Disk
erstellen 90
für das Wiederherstellen von Protection Center
verwenden 87
testen 91
Symantec Support
zur Lösung von Problemen verwenden 115
SymConnect-Forum
zur Lösung von Problemen verwenden 115
SymWISE
zur Lösung von Problemen verwenden 114
Systemprotokolle
Anzeigen 99

- Bereinigung 99
- zur Lösung von Problemen verwenden 114
- Systemsteuerung
 - Info 106
 - Netzwerkeinstellungen angeben von 109
 - Protection Center-Software aktualisieren 107
 - SPC_Admin-Kennwort ändern 108
 - SPC_Admin-Konto 107-108
 - Windows Update-Server-Speicherort angeben 111
 - Windows-Betriebssystem aktivieren über 111
 - zugreifen 107

U

- Unterstütztes Produkt
 - Aktivieren 31, 37
 - Aktiviert 36
 - Aktivierte mehrere Mandanten erkennen 35
 - Deaktivieren 31
 - deaktivieren 38
 - entfernen 38
 - Erforderliche Host-Einstellungen für das Hinzufügen des Tenants eines Produkts mit mehreren Tenants 33
 - erforderliche Hosteinstellungen zum Hinzufügen 33
 - Erkennen 31, 35
 - Erneut aktivieren 31, 39
 - Erweiterte Host-Einstellungen für das Hinzufügen 33
 - Hinzufügen 31-32
 - Info 29
 - Instanz aktivieren 37
 - Instanz deaktivieren 38
 - Integrieren 30
 - Liste 36
 - Tenant des Multi-Tenants hinzufügen 32
 - Verfügbar 36
 - Verwalten 36
 - verwalten 131
 - Verwaltungsoptionen 36
 - zugreifen 131
 - Zusätzliche Mandanten aktivieren 35

W

- Wiederherstellen
 - Backup-Datei-Kennwortschutz 86
 - Daten aus Backup-Dateien 87

- Info 84
- Symantec Recovery Disk 87
- Wiederherstellungsdatenträger erstellen 90
- Wiederherstellungsdatenträger testen 91

Workflow

- "Endgerät verschieben" 159
- "Endgerät verschieben", Beschreibung 164
- "Endgerät verschieben", Einstellungen 164
- "NationalThreatLevel" 160
- "NationalThreatLevelMonitor", Beschreibung 166
- "NationalThreatLevelMonitor", Einstellungen 166
- "Virendefinitionen auf Endgerät aktualisieren" 160
- "Virendefinitionen auf Endgerät aktualisieren", Beschreibung 163
- "Virendefinitionen auf Endgerät aktualisieren", Einstellungen 163
- "Virendefinitionen und Scan-Endgerät aktualisieren" 160
- "ZeroDayVulnerability" 160
- "ZeroDayVulnerabilityMonitor", Beschreibung 166
- "ZeroDayVulnerabilityMonitor", Einstellungen 166
- Aktionseinstellungen konfigurieren 154
- Details 156
- Diagramm "Meine Aufgaben" 157
- in Protection Center beginnen 154
- Info 151
- Quarantäne-Endgerät, auf zugewiesene Aufgaben reagieren 162
- Quarantäne-Endgerät, Beschreibung 161
- Quarantäneendgerät 159
- Quarantäneendgerät, Einstellungen 161
- Status überwachen 155
- verfügbar in Protection Center, Liste von 159
- Verwaltungseinstellungen konfigurieren 154
- Virendefinitionen und Scan-Endgerät aktualisieren, Beschreibung 164
- Virendefinitionen und Scan-Endgerät aktualisieren, Einstellungen 165
- Zu verwendender Prozess 152